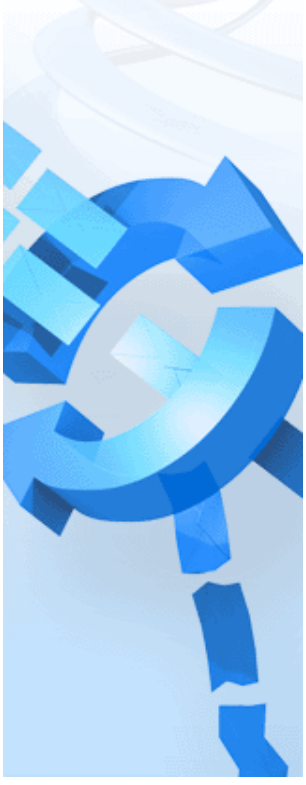
WinDeveloper Software

WinDeveloper IMF Tune



IMF Tune v7.0 Server

Contents

1. Welcome 4
2. Key Features 5
3. System Setup 7
3.1 Minimum Requirements 8
3.2 Setup Exchange 2003 Intelligent Message Filter 9
3.3 Setup Exchange 2007/2010/2013 Content Filter Agent 10
3.4 Installing/Removing Forefront Protection 2010 for Exchange 11
3.5 Installing WinDeveloper IMF Tune 12
4. Email Processing Configuration 13
4.1 Email Handling 16
4.1.1 SCL Handling Action Configuration 19
4.1.2 SCL Range 20
4.1.3 Actions 21
4.1.4 Grabbing a Copy of Accepted Emails 22
4.1.5 Rerouting Emails to a Central Mailbox 23
4.1.6 Email Modifications 24
4.1.7 Customizing Insertion of SCLs in the Email Subject 25
4.1.8 Headers Inserted in Accepted/Rerouted Emails 27
4.1.9 Overriding the Default SMTP Rejection Text 28
4.2 Archiving/Quarantine 29
4.2.1 Archiving Profiles 30
4.2.2 Choosing an Archive Directory Path 32
4.2.3 Archived Emails Modifications 33
4.2.4 Headers Inserted in Archived Emails 34
4.2.5 Publishing Emails to Quarantine 35
4.3 Logging 36
4.3.1 Logging Profiles 37
4.3.2 Log File Fields 39
4.4 Auto-Replies 40
4.4.1 Auto-Reply Profiles 41
4.5 Disk Maintenance 43
4.5.1 Archive/Quarantine Maintenance 44
4.5.2 Logs/Reports Maintenance 50
4.6 Quarantine 55
4.7 Auto-Whitelist Senders 56
4.7.1 Configuring Sender Auto-Whitelisting 57
4.7.2 Auto-Whitelist Exceptions 59
4.7.3 Reporting Auto-Whitelist Matches 60
4.7.4 Extracting the List of Auto-Whitelisted Addresses 62
4.8 Working with Whitelists 65
4.8.1 Accept Senders and Accept Recipients Lists 65
4.8.2 Accept Subjects and Accept Bodies Lists 70
4.8.3 Accept IPs 77
4.8.4 Accept Attachments 82
4.9 Working with Blacklists 87
4.9.1 Foreign Spam Blacklist 88
4.10 DNS List Filtering (Exchange 2007/2010/2013) 89
4.10.1 DNS Server Configuration 90
4.10.2 DNS IP Lists 91

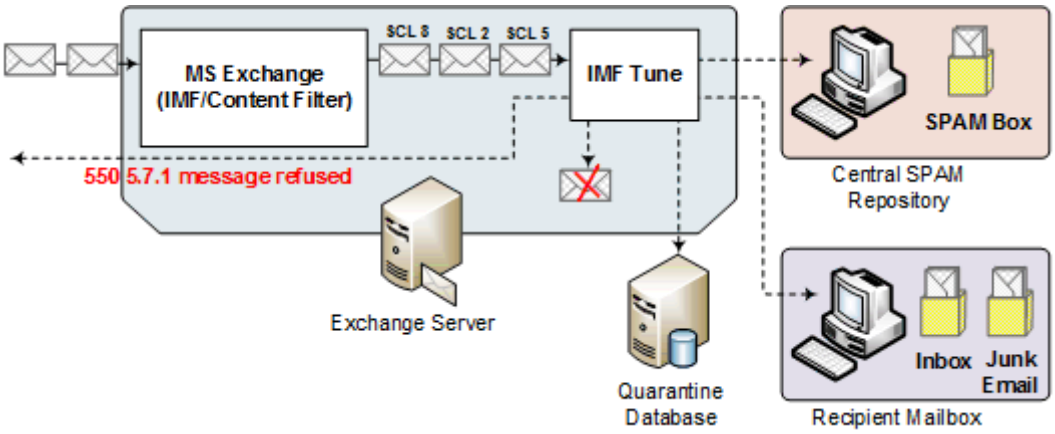
4.10.3 DNS URI Lists 97
4.10.4 DNS List Reporting 102
4.11 Simple SCL Rules 103
4.11.1 Working with Simple SCL Rules 104
4.11.2 Adding/Editing New SCL Mappings 105
4.11.3 SCL Mapping Configuration 106
4.12 Advanced SCL Rules 116
4.12.1 Working with Advanced SCL Rules 117
4.12.2 Adding Advanced SCL Rules 118
4.13 External SCL Rules 132
4.13.1 Working with External SCL Rules 133
4.13.2 External File Format 138
4.13.3 External File UNC Path 139
4.13.4 External File Access Permissions 140
4.14 Constructing Search Expressions 143
4.14.1 Basic Expression Syntax 144
4.14.2 Exact Matching 145
4.14.3 Whole Word, Word Start/End Matching 146
4.14.4 Punctuation Handling 147
4.14.5 Minimum Keyword Length 148
4.14.6 AND OR NOT Operators 149
4.14.7 Invalid and Illegal Operator Sequences 151
4.14.8 Working with the Expression Builder 152
4.15 Keyword Reporting 154
4.15.1 Understanding the Keyword Report 156
4.16 Exchange/Forefront SCLs (Exchange 2007/2010/2013) 159
4.16.1 Customizing SCL -1 Handling 160
4.17 Unprocessed Emails (Exchange 2003 Only) 162
4.18 Exchange System Manager Anti-Spam Settings (Exchange 2003 Only) 163
4.18.1 Exchange Intelligent Message Filter Settings 164
4.18.2 Exporting Exchange Anti-Spam Settings 167
4.19 Details 169
4.20 Product Version/Disabling IMF Tune 170
5. Licensing WinDeveloper IMF Tune 171
5.1 Licensed Email Domains 172
6. Contacting WinDeveloper 174
Annex A – Exchange 2003 Intelligent Message Filter 175
A.1 Installing IMF 176
A.2 Configuring IMF 178
A.3 Enabling IMF v2 (Exchange 2003 SP2) 180
A.4 Enabling IMF v1 (Exchange 2003 SP1 and Earlier) 182
A.5 Enabling the Junk Email Folder 183

1. Welcome

WinDeveloper IMF Tune enables the Microsoft Exchange built-in spam filters and Forefront Protection 2010 for Exchange to unleash their full power.

Today all Exchange versions from 2003 to 2013 come complete with free anti-spam filtering. The powerful underlying engine is bottled in an interface exposing minimal functionality. IMF Tune changes this, transforming the filter into a full featured anti-spam solution.

Even if running Forefront Protection 2010 for Exchange, IMF Tune brings significant improvements. Additional spam filters, email moderation from the browser, reporting, and a much more effective configuration interface are some of the enhancements.



2. Key Features

Exchange 2003/2007/2010/2013 Support - Extensive Exchange version support including all of Exchange 2003, 2007, 2010 and 2013. Server platform support includes Windows 2003, 2008, 2008 R2, 2012, 2012 R2 and Small Business Server 2003/2008/2011.

Multiple SCL Threshold Configuration - Configure individual SCL ratings or ranges with a unique set of options including archiving, logging, attachment stripping, subject tagging, auto-replies, rerouting, rejection, deletion and more.

Sender Auto-Whitelisting - Let IMF Tune automatically discover the foreign contacts your users are exchanging emails with. Subsequent emails are automatically whitelisted relieving you from manual configuration.

DNS White/Block List Filters - Subscribe to DNS List providers to block/allow emails or just raise/lower the current spam rating (only for Exchange 2007/2010/2013)

Whitelisting/Blacklisting - At the server maintain global and per user white/black lists. Identify legitimate emails and spam by IP, sender, recipient, subject, any email header, body keywords, attachment names and more.

Central Email Quarantine - Retain copies of blocked emails on disk. Optionally publish Quarantines to an SQL Database. Let IMF Tune automatically manage the email archive, compressing, backing-up and deleting old emails.

Resubmit Blocked Emails from Browser - Install the included IIS Web Moderator/Reporting interface for the Quarantine system to be accessible from anywhere. The moderator supports the latest version of all major browsers.

Filter Performance Graph/Chart Reports - From the browser, access real-time reports to monitor the filtering effectiveness. See how emails are being rated, the rejection rate, the list of top spam sources and many other reports.

Integrate any Anti-Spam Filter into Exchange - Run spam filtering on ANY platform, firewall appliance, external service provider without losing Exchange integration.

CSV Logging - Keep record of each email, including any actions applied, the source IP, addresses, subject and SCL rating as a concise audit trail.

Multiple Condition/Exception Filtering Rules - Construct rules by combining multiple conditions and exceptions to accurately identify legitimate and spam emails.

Insertion of SCL Ratings in Subject - Expose SCL ratings to all users from the server. Insert an SCL subject tag or add a custom header.

Fine Tune SCL Assignments - Influence the email filtering logic. Identify keywords that should lead to higher or lower SCL ratings.

Attachment Filtering - Block/Allow email delivery by attachment name or attachment media type.

Foreign Spam, NDR Spam, SMTP Protocol Command Data - Let IMF Tune dig all the information for you to express the most effective email filtering criteria.

Spam Rerouting to Mailbox or Public Folder - Retain all emails within a single repository. Eliminate disk archiving and access filtered spam from Outlook.

3. System Setup

The IMF Tune installation is made up of two components:

1. IMF Tune Server for Exchange 2003, 2007, 2010 and 2013.
2. IMF Tune Moderator/Reporting Web Interface

The Web interface component is optional. In fact IMF Tune can be run without it ever being installed, but of course we would be missing all the functionality this interface delivers.

If installing IMF Tune for the first time we recommend focusing on the IMF Tune server installation/upgrade first. Completing this step, we have a fully functional IMF Tune delivering all the filtering functionality. The Web component installation can be completed later, without causing any disruption.

The primary focus of this manual is the installation and configuration of the IMF Tune Server. Even though this manual visits the Moderator/Reporting functionality in various sections, a full discussion of the Web component installation, configuration and usage is not included here. Instead the Web component has a dedicated document. Look for this under the IMF Tune application program group.

3.1 Minimum Requirements

1. **Platform Support** – The IMF Tune server is installed on the Exchange server machine. Exchange versions 2003, 2007, 2010 and 2013 are supported. The following is the list of supported platform/Exchange server combinations:

   Exchange 2003 SP2
   - Windows 2003 (x86), SBS 2003 (x86)

   Exchange 2007 [1]
   - Windows 2003 (x64), Windows 2008/2008 R2 (x64), SBS 2008 (x64)

   Exchange 2010 [1]
   - Windows 2008/2008 R2 (x64), SBS 2011 (x64)

   Exchange 2013 [2]
   - Windows 2008 R2 (x64), Windows 2012 (x64), Windows 2012 R2 (x64)

   [1] IMF Tune must be installed on the Edge or Hub transport server roles. The Exchange Content Filter or Forefront Protection 2010 for Exchange must also be installed.

   [2] IMF Tune must be installed on the Exchange 2013 Mailbox Server. The Exchange Content Filter must also be installed.

2. **.NET 2.0 Framework SP2**
   Note: On Windows 2012 and later, add the **.NET Framework 3.5 Feature** from the Server Manager. This includes .NET Framework 2.0 satisfying this installation requirement.

3.2 Setup Exchange 2003 Intelligent Message Filter

Microsoft released two versions of the Exchange 2003 Intelligent Message Filter (IMF), the latest being IMF v2. Both are supported, but IMF v2 is recommended for the best filtering results.

IMF v2 is included as part of Exchange 2003 SP2. This means that once SP2 is installed, IMF is ready to be enabled.

IMF v1 was the first filter version available for Exchange 2003 systems preceding SP2. This used to be available from the Microsoft download center and deployed as a separate installation step.

It is very important to remember that IMF v1 should never be installed on Exchange 2003 SP2 machines. Doing so is likely to break IMF leading it to stop filtering any spam.

IMF must be installed before IMF Tune. It is also recommended to deploy IMF and IMF Tune in separate steps. In this manner one can make sure that IMF is functioning correctly before IMF Tune is deployed. This simplifies troubleshooting in case of problems. For further details on the Exchange Intelligent Message Filter please refer to Annex A.

3.3 Setup Exchange 2007/2010/2013 Content Filter Agent

The Content Filter Agent forms part of a set of anti-spam transport agents that ship with Exchange 2007/2010/2013. These must be run on a server having the Edge or Hub transport server role.

The Edge server installation automatically installs the anti-spam agents. However in case of Hub Transport servers, the agents must be installed manually from the command shell.

In Exchange 2013, unlike earlier versions, there is no distinct Hub Transport Server role. Instead the Hub Transport is included within the Mailbox Server role. Thus in Exchange 2013 IMF Tune is installed on servers running the Mailbox Server role.

The installation script is located under:
<Exchange Server dir.>\Scripts\install-AntispamAgents.ps1

1. On the Hub transport server machine, from the Exchange program group, open the Exchange Management Shell.
   Note: If User Access Control is enabled make sure to run the Shell with *'Run as Administrator'*.

2. Change the directory to:
   <Exchange Server dir.>\Scripts

3. Run> .\install-AntispamAgents.ps1
   Note: When running the installation script include the leading ".\" to the command. Otherwise the installation may fail.

4. Restart the Microsoft Exchange Transport service

3.4 Installing/Removing Forefront Protection 2010 for Exchange

In Exchange 2007/2010 we can run IMF Tune together with Forefront Protection 2010 for Exchange anti-spam. Both the built-in and the Forefront Content Filters are supported, so we can employ any of the two.

For details on how to install Forefront refer to the product documentation. Here we highlight some important points:

- By default the Forefront 2010 installation does not enable the anti-spam component. Enablement can be done from the Forefront installation wizard or from the Forefront Management console.

- It is simpler to install and enable Forefront anti-spam before IMF Tune is installed. The IMF Tune installation automatically detects Forefront anti-spam and initializes itself with the correct transport agent priority.

- If Forefront anti-spam is enabled **after** that IMF Tune is installed, we may need to refresh the transport agent priority. When such a system change is done, re-open the IMF Tune configuration. On startup the configuration performs automatic problem detection. If the agent priority needs refreshing a warning will be raised together with instructions on how to fix the problem.

- Uninstalling Forefront, or disabling Forefront anti-spam, leaves Exchange without any active Content Filter. In this case we need to enable the built-in Content Filter manually. Details on how to do this is available from Going Back from Forefront 2010 Anti-Spam to the Exchange Content Filter

3.5 Installing WinDeveloper IMF Tune

Installing the IMF Tune server cannot be any simpler. Given that the necessary requirements discussed above are satisfied, it is just a matter of clicking Next, Next, Next to complete the installation Wizard.

Unless the default is changed, the application will be installed to:
<Program Files>\WinDeveloper IMF Tune

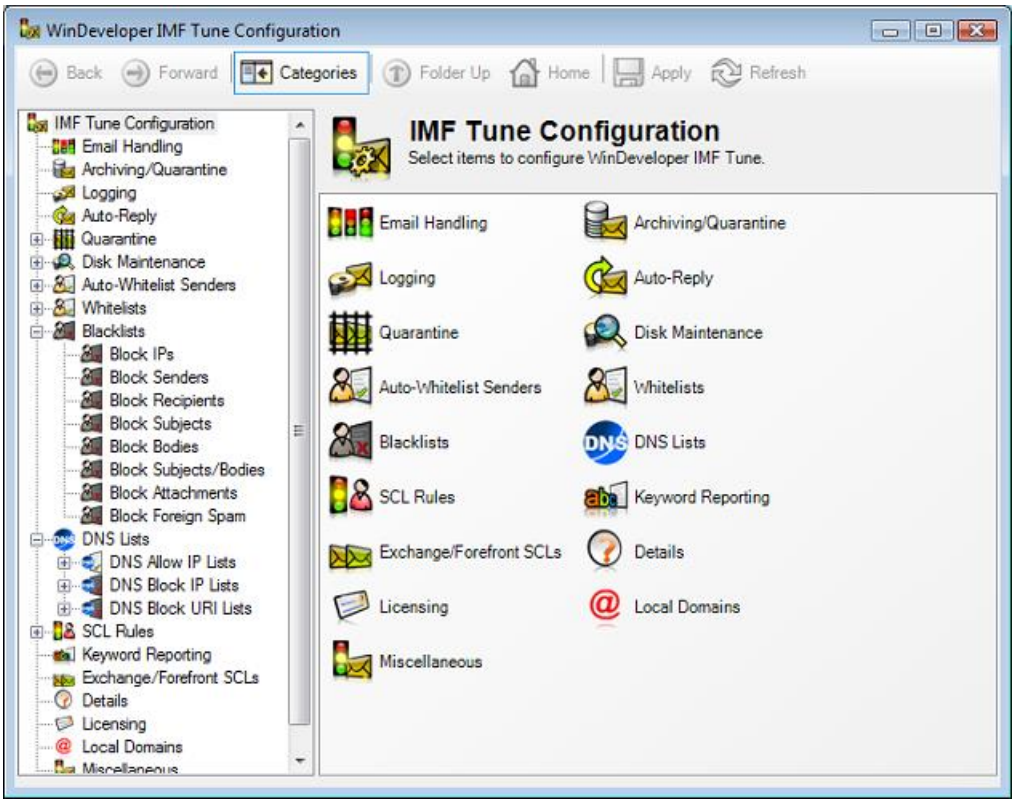
The installation will not cause any service restarts or downtime. Once completed IMF Tune will be ready to process emails.

4. Email Processing Configuration

The IMF Tune configuration is available from the application program group at:
Windows Start | Programs | WinDeveloper IMF Tune | IMF Tune

The configuration is organized in two panes. The left pane shows the main configuration categories while the right pane shows the options for the currently selected category.

The exact set of configuration categories depends on the MS Exchange version. The **Unprocessed Emails** and **Exchange System Manager** categories are only available when running Exchange 2003. Likewise the **DNS Lists** and **Exchange/Forefront SCLs** categories are only available when running Exchange 2007/2010/2013. Here is what the IMF Tune configuration looks like in Exchange 2007/2010/2013.



The **Email Handling** category provides a selection of actions from Accepting, Rerouting, Deleting and Rejecting emails based on the final SCL ratings.

The **Archiving/Quarantine** category allows us to archive emails to disk and to also Quarantine emails for review from the IMF Tune Web Moderator.

The **Logging** category exposes the configuration for enabling detailed CSV logging of processed emails.

At the **Auto-Reply** category, automated email responses may be configured to be fired for specific SCL ratings.

The **Quarantine** category groups connectivity and other administrative options for managing the Quarantine/Reporting database server.

The **Disk Maintenance** category allows for automating the management of disk archives, log files and the quarantine/reporting database. This includes the ability to schedule automatic backups and purging of email information older than the specified age limit.

The **Auto-Whitelist Senders** category controls the automatic discovery and whitelisting of foreign contacts with whom local users are exchanging emails.

The **Whitelists** category groups the IP, Sender, Recipient, Subject, Body, combined Subject/Body, and Attachment whitelisting functionality. Whitelisting overrides any previously assigned SCL making sure the email is not classified as spam.

The **Blacklists** support the same categories as the Whitelists with the addition of Language blacklisting. Blacklisting identifies emails that are to be handled as spam.

The **DNS Lists** category (only available in Exchange 2007/2010/2013) provides support for DNS blacklists and whitelists. The sender IP and URIs extracted from the email body are checked against the DNS Lists configured here.

The **SCL Rules** category provides finer control on SCL assignments. From here one can construct rules combining multiple conditions and exceptions to accurately identify legitimate and spam emails. The rules can test all kind of email properties including headers, bodies, addresses, IPs etc. Once a match is found the current SCL value may be incremented, decremented, or replaced by a new value.

The **Keyword Reporting** category provides the necessary functionality to generate a detailed HTML report on all emails matching any of the whitelists, blacklists and SCL Rules. In this manner one can see exactly how the configuration at IMF Tune is influencing the final SCL ratings assigned to each email.

The **Exchange/Forefront SCLs** category (only available in Exchange 2007/2010/2013) determines how IMF Tune is to handle emails having an initial SCL -1 rating. This is especially useful when running Forefront Protection 2010 for Exchange.

The **Unprocessed Emails** category (only available in Exchange 2003) caters for any emails the MS Exchange IMF leaves unhandled. From here IMF Tune may be instructed to scan emails that would otherwise go through unprocessed.

The **Exchange System Manager** category (only available in Exchange 2003) exposes various other anti-spam settings. This is a read-only view of the options available from the Exchange 2003 System Manger console. It includes the Intelligent Message Filter settings, Sender ID settings and the various Exchange 2003 out-of-the-box options for Connection, Sender and Recipient filtering.

The **Details** category provides the necessary space for administrative notes. In this manner an administrator can insert comments to better keep track of configuration changes.

The **Licensing** category shows the type of license currently in place. Some examples include time limited evaluation licenses, user limited licenses and unlimited users licenses.

The **Local Domains** category configures the list of SMTP domains Exchange mailboxes are using. This information is required for some features (such as Sender Auto-Whitelisting) to work.

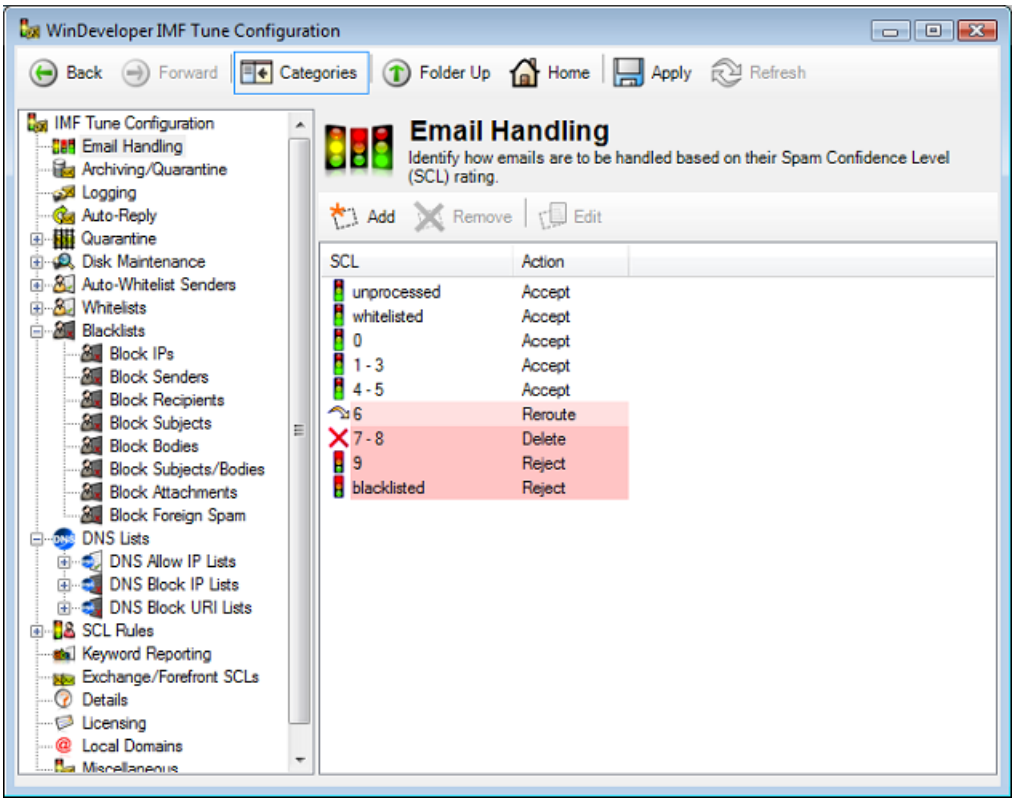
The **Miscellaneous** category gives quick access to product version and contact information.

4.1 Email Handling

Under the IMF Tune configuration, the Email Handling category provides a set of actions to be applied to emails based on their SCL rating.

An SCL is assigned to an email by the Content Filter/Intelligent Message Filter/Forefront as a means to classify its likeliness of being spam. The higher the SCL value the more likely the email to be spam. IMF Tune processing may change this rating reaching the final SCL.

The IMF Tune Email Handling category presents a list interface. Each list entry specifies actions to be applied for a specific range of SCL values.

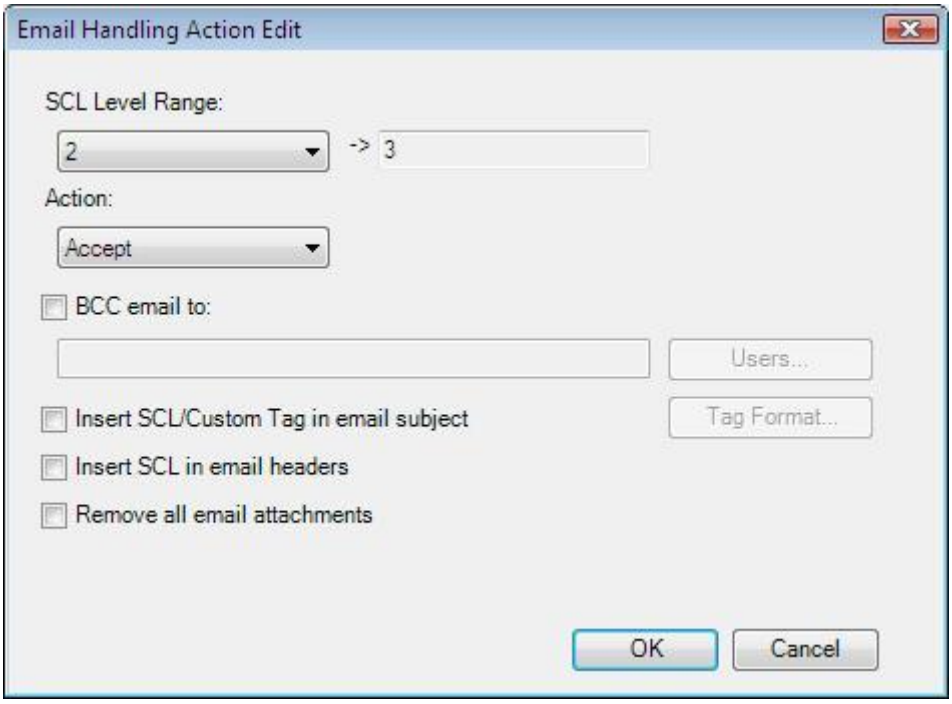


In this case email handling for unprocessed, whitelisted, blacklisted and SCLs 0, 1-3, 4-5, 6, 7-8 and 9 are configured. The icons and Action column show that four different actions are configured:

- Unprocessed, whitelisted and SCLs 0-5 are set to Accept
- SCL 6 is set to Reroute
- SCLs 7-8 are set to Delete
- SCL 9 and blacklisted are set to Reject

Note how ranges with action set to Accept have a white background. Other actions have a light shade of red signifying the increased level of action severity.

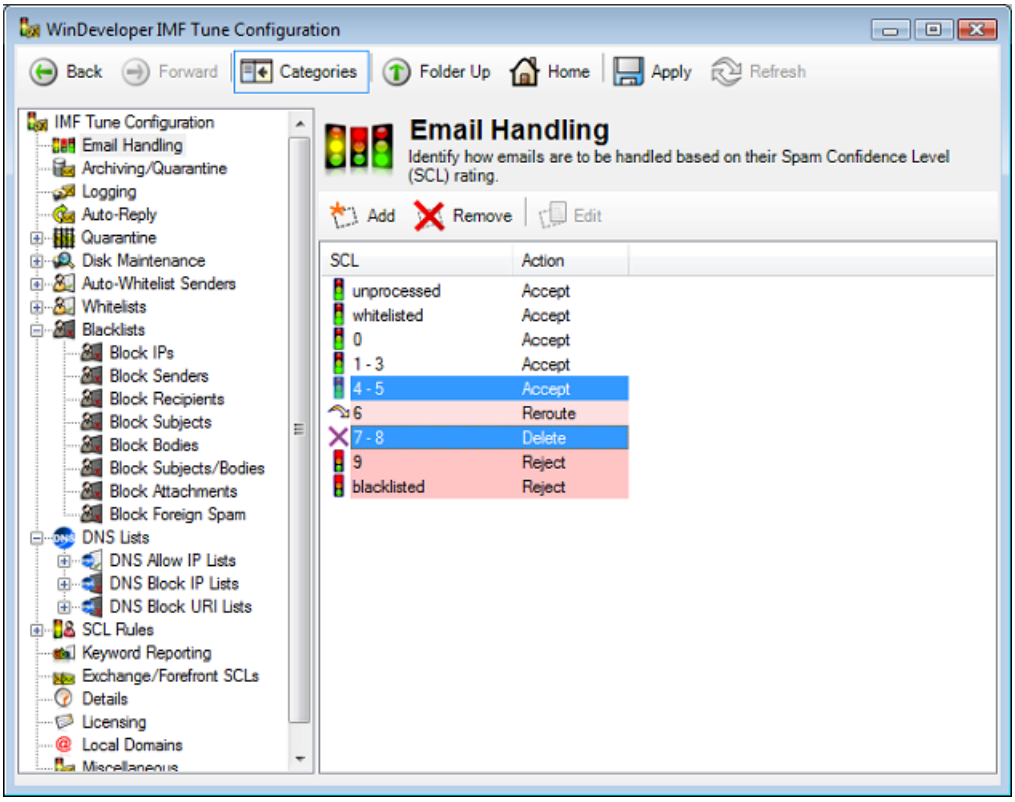
Working with the list interface is fairly trivial. To specify actions for a new SCL range, click the Add button. This opens the Email Handling Action Edit dialog.



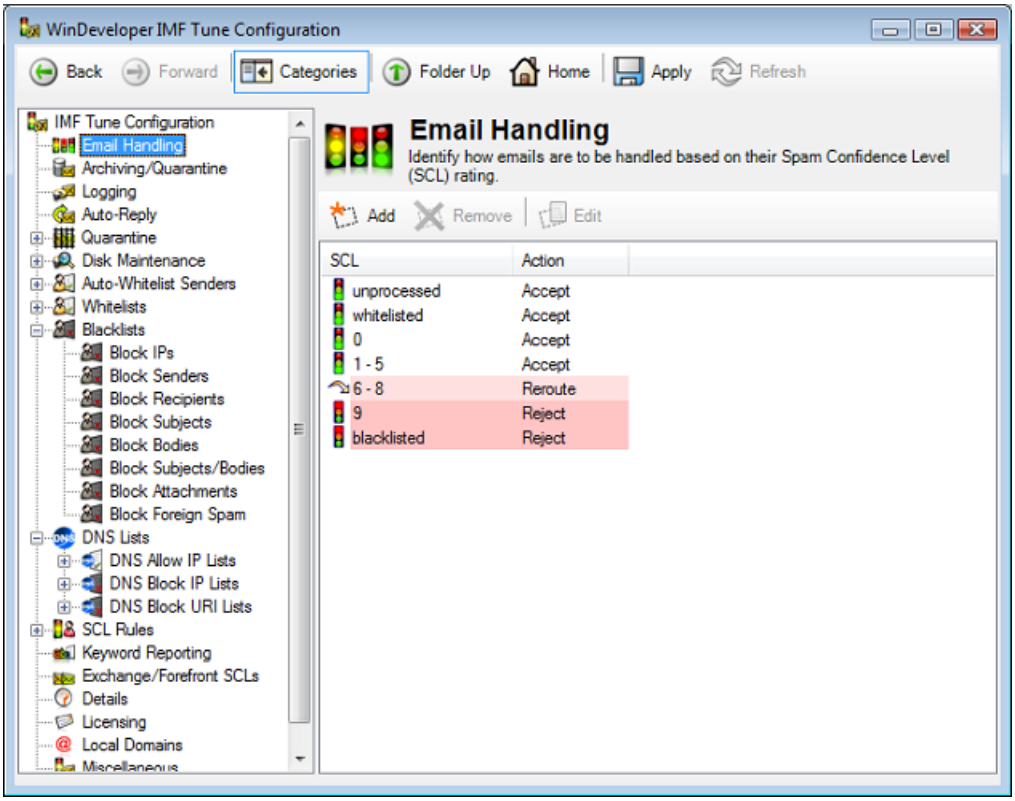
This dialog presents a set of operations that can be applied to an Email with matching SCL rating. Refer to SCL Handling Action Configuration for more details on each of these options.

To edit email handling options for an already defined SCL range, select the entry from the list and click on Edit. Note that we may only edit one entry at a time.

To remove email handling options select the SCL ranges and click on the Remove button. Note that entries for unprocessed, whitelisted, blacklisted and SCL 0 cannot be removed.

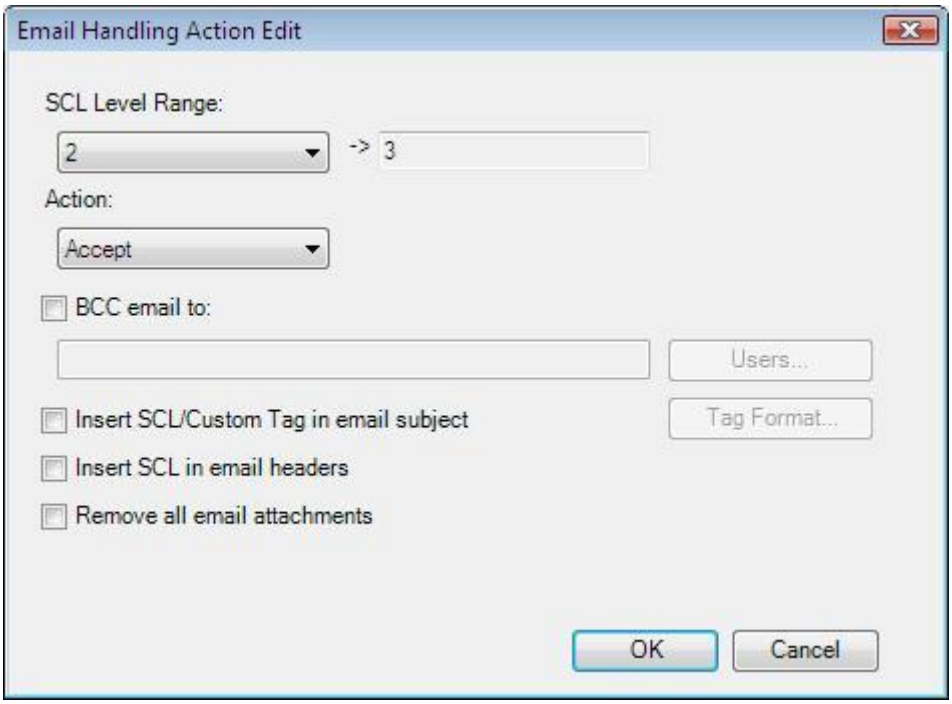


On removing an SCL range, the range that immediately precedes it, is extended to cover the gap generated by the deletion.



4.1.1 SCL Handling Action Configuration

Adding or editing actions for an SCL range is done through the SCL Handling Action dialog.



It provides the following configuration options:

- An SCL range for which these settings are to be applied.
- An action to be performed on the emails.
- A set of additional email modifications.

The actions and modifications configured here are applied directly to incoming emails. Once the Exchange Content Filter completes its processing, IMF Tune takes over and performs its own spam filtering. Combining the outcome of the two filtering stages gives us the final SCL rating. Thus the Email Handling configuration with matching SCL range is identified and applied.

4.1.2 SCL Range

The configuration only enables the setting of the lower SCL range limit value. The upper range limit is automatically set. This is done by referring to the already configured SCL ranges and setting it so as not to leave gaps.

IMF Tune SCL ranges are always inclusive of the lower and upper limits. This means that a range 3 to 5 includes emails assigned any of the SCL values out of 3, 4 and 5.

The lower SCL range limit is selected from a combo box. This lists all available values. SCL values that have already been set as the lower limit for other entries are excluded.

IMF Tune gives special handling to unprocessed, whitelisted, blacklisted and SCL 0. These are always present and cannot be removed. For this reason their SCL range is not editable and the combo box is grayed.

4.1.3 Actions

At the Email Handling Action dialog, one out of four possible actions must be set. These are:

Accept – Permits the email to reach the recipient mailbox.
Reroute – Redirects the email to the specified address.
Delete – Deletes the email blocking it from reaching its destination.
Reject – Rejects the email returning an SMTP error response to the sender.

On accepting or rerouting, the email may still be deposited to the Junk Email folder. The IMF configuration to deposit emails to this folder is not overridden. In fact Accept is the correct IMF Tune action when emails are required to finish into the end-recipient Junk Email folder.

The set of possible actions configurable depend on the current SCL range setting. This is so as to enforce the rule that the higher the SCL, the stricter the Action. Consider SCL 6 is configured to reroute emails. In that case on configuring SCL 7 only reroute, delete or reject are possible. It doesn't make sense to first Reroute emails with SCL 6 and then Accept emails with higher SCL ratings.

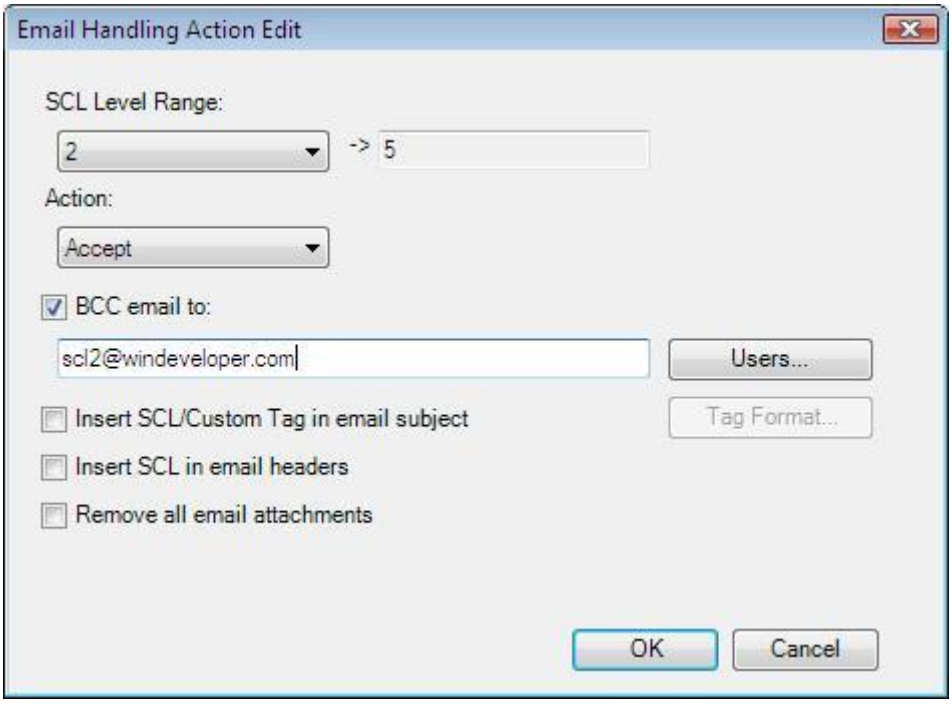
The action for unprocessed, whitelisted and SCL 0 is fixed to Accept. These classifications are meant to identify legitimate emails. Thus any action other than Accept would cause loss of valuable email.

Depending on the type of action selected, the configuration will automatically provide a set of additional options. The sections that follow discuss these options in more detail.

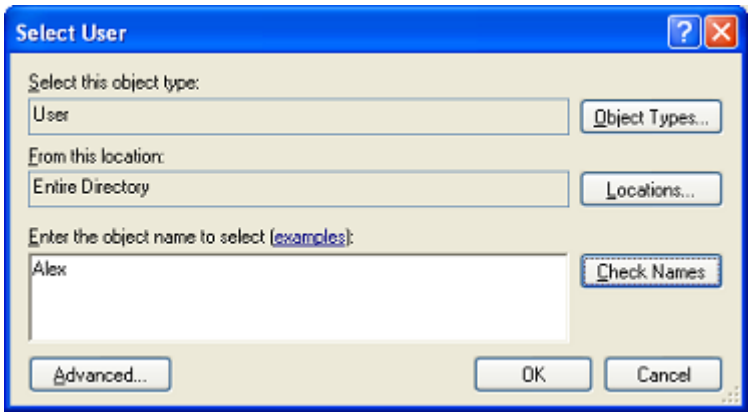
4.1.4 Grabbing a Copy of Accepted Emails

IMF Tune allows us to grab a copy of the emails reaching recipient mailboxes. This can be useful when analyzing the performance of specific SCL ratings.

On selecting the Accept action, the 'BCC Email to' option is exposed. Set the checkbox to enable this functionality. We may then specify the address to which emails are to be copied. Since the new address is BCCed, the email content is unchanged. Thus emails may be analyzed unobtrusively.



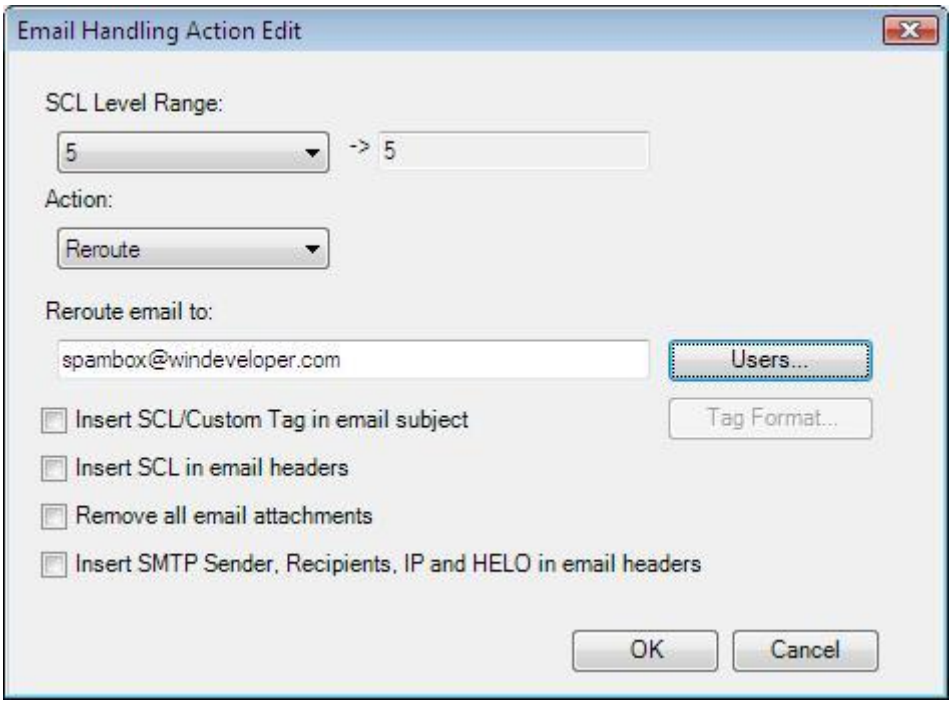
We can either type the BCC address directly or click on Users to lookup an address from Active Directory.



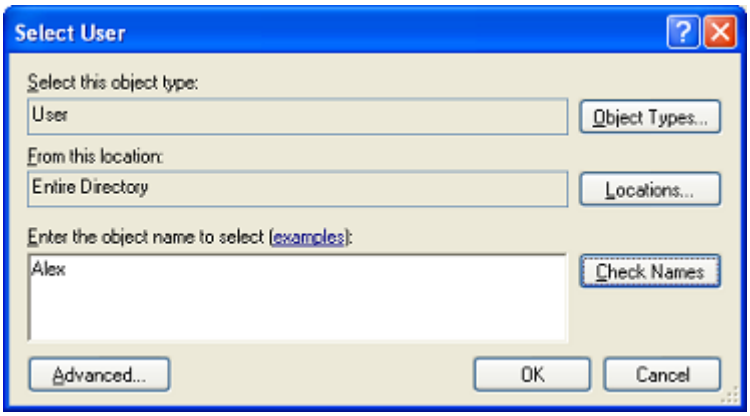
In the Select User dialog that opens, enter a user name and click on Check Names to resolve the email address. Click OK to set this as the BCC email address.

4.1.5 Rerouting Emails to a Central Mailbox

The Reroute action diverts email delivery to a central mailbox. Selecting Reroute, will enable the 'Reroute email to' edit box and the Users button. Enter a valid SMTP address to which emails are to be rerouted.



Otherwise click on Users to lookup an address from Active Directory.



In the Select User dialog that opens, enter a user name and click on Check Names to resolve the email address. Click OK to set this as the reroute email address.

4.1.6 Email Modifications

The Email Handling Action dialog also enables the selection of additional email modifications. These options are only available in case Accept or Reroute actions are selected. Since Delete and Reject completely block email delivery configuring modifications is useless as these would be lost anyway.

If the action is set to Accept or Reroute the following email modifications are possible:

- Insert SCL in email subject
- Insert SCL in email headers
- Remove all email attachments

In case of Reroute the following is also possible:

- Insert SMTP Sender, Recipients, IP and EHLO in email headers

Email modifications are disabled for unprocessed emails. Also whitelisted and SCL 0 do not allow the removal of email attachments. These ratings are meant to identify legitimate emails. Thus modifications should be kept to a minimum.

Inserting SCLs in the email subject can be very useful when dealing with spam. Emails ending in the recipient junk email folder could then be sorted by SCL rating. In this manner one can quickly review all trapped email whose SCL is lowest.

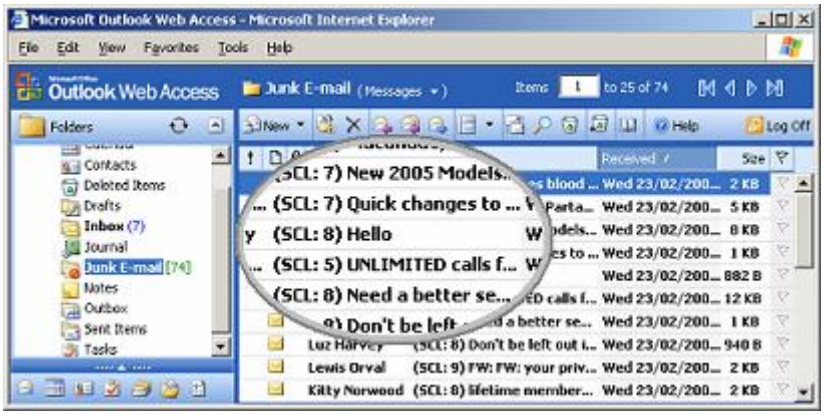
Exposing SCL values is also useful when fine tuning configuration settings. We can analyze the performance of a set of settings in terms of false positives/negatives and then apply adjustments to the SCL thresholds. Another way of doing this is to use SCL based logging which is discussed later in this manual.

Removing email attachments reduces the waste in storage caused by spam. Retaining spam in Junk Folders for a long time may stretch the mailbox size requirements. This option removes any email attachments and images reducing this problem.

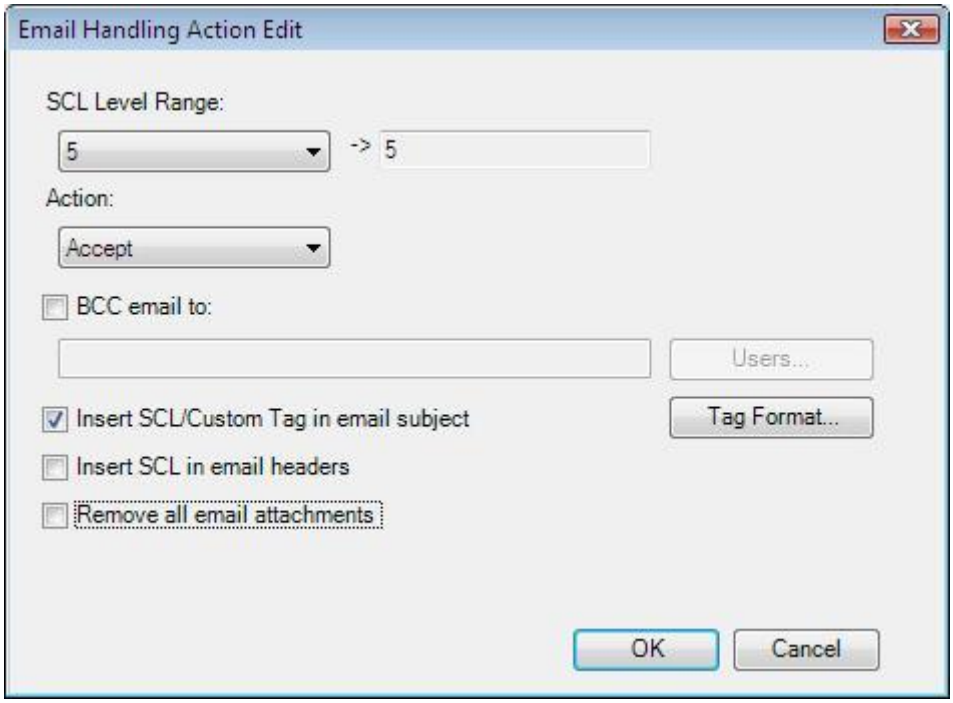
Insertion of SMTP headers is only available when rerouting emails (and on archiving emails which is discussed later in this manual). This option discloses the complete list of SMTP recipients including BCCs. This information is normally considered to be confidential. Thus the option is disabled for the Accept action.

4.1.7 Customizing Insertion of SCLs in the Email Subject

When performing Accept or Reroute actions, it is possible to insert the SCL rating into the email subject.

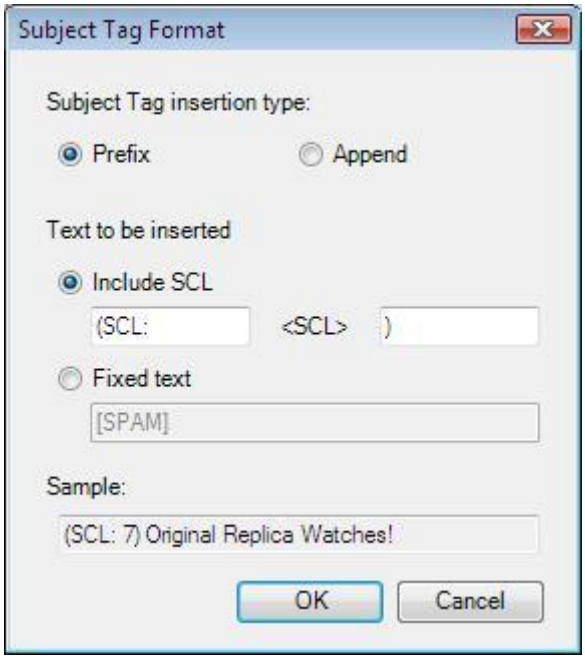

Microsoft Outlook Web Access - Microsoft Internet Explorer
Outlook Web Access
Junk E-mail
(SCL: 7) New 2005 Models...
(SCL: 7) Quick changes to ...
(SCL: 8) Hello
(SCL: 5) UNLIMITED calls f...
(SCL: 8) Need a better se...
Lewis Orval (SCL: 9) FW: FW: your priv...
Kitty Norwood (SCL: 8) lifetime member...

IMF Tune provides a number of customization options in this area. Start by selecting the 'Insert SCL/Custom Tag in email subject' checkbox:



By default this will prefix the subject with the text:
(SCL: <n>)

Here <n> is the SCL rating assigned to the email. To customize this, click on the Tag Format button.



From here we can choose between prefixing and appending the inserted text to the subject. We may also choose to insert a fixed text phrase rather than a tag containing the SCL rating.

This type of customization can be very useful in case Outlook client rules are in place at the recipient mailboxes. Very often these rules are configured to match the initial part of the email subject. Thus prefixing the subject with the SCL rating could break such rules. Customizing the insertion so as to append rather than prefix the subject, resolves this type of issue.

At the bottom of the dialog, we can immediately see an example of the tagging as applied to a sample email subject.

4.1.8 Headers Inserted in Accepted/Rerouted Emails

The following table lists the headers that can be inserted into emails when the action specified is Accept or Reroute.

Header	Description	Action
x-scl	The email SCL rating.	Accept, Reroute
x-smtp-ip	The email sender IP.	Reroute
x-smtp-helo	The SMTP HELO/EHLO host name.	Reroute
x-smtp-sender	The SMTP FROM originator address.	Reroute
x-smtp-receiver	A comma separated list of SMTP RCPT TO recipient addresses.	Reroute

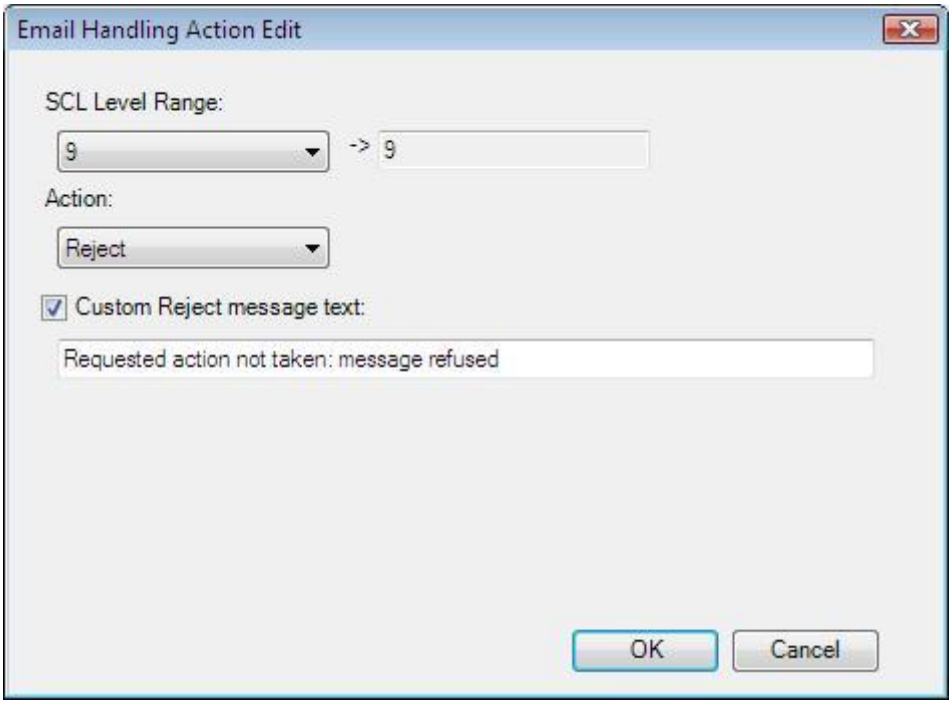
4.1.9 Overriding the Default SMTP Rejection Text

IMF Tune also provides the ability to immediately reject emails at SMTP protocol level. By default the following SMTP rejection response is issued:

“550 5.7.1 Requested action not taken: message refused”

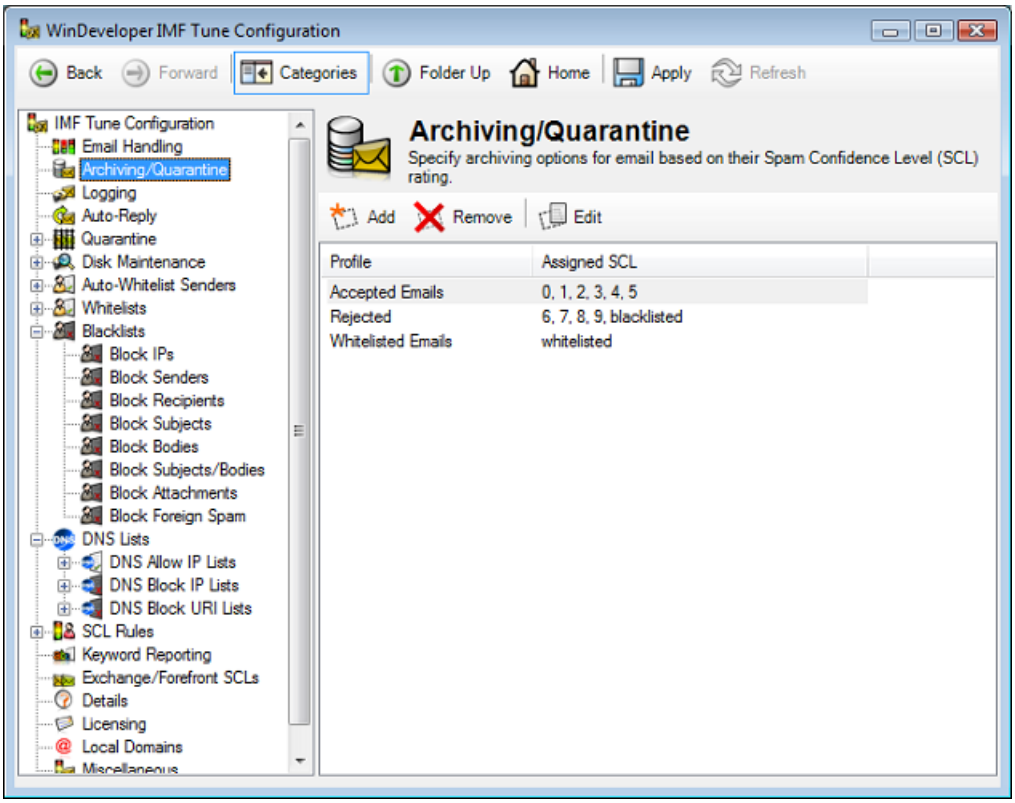
The default rejection reason is very generic. It is sometimes useful to change this text so as to supply a more informative response. When doing so, typically we would consider the case where some legitimate email is being rejected. In such a case we might want to supply information enabling the sender to report the problem in some other way, for example by phone.

To customize the rejection response, select the ‘Custom Reject Message Text’ checkbox and fill in the new message text.



4.2 Archiving/Quarantine

IMF Tune disk archiving saves a copy of processed emails to disk. In addition it also gives the option to publish a copy of the email to a central database for Moderation and Reporting purposes.



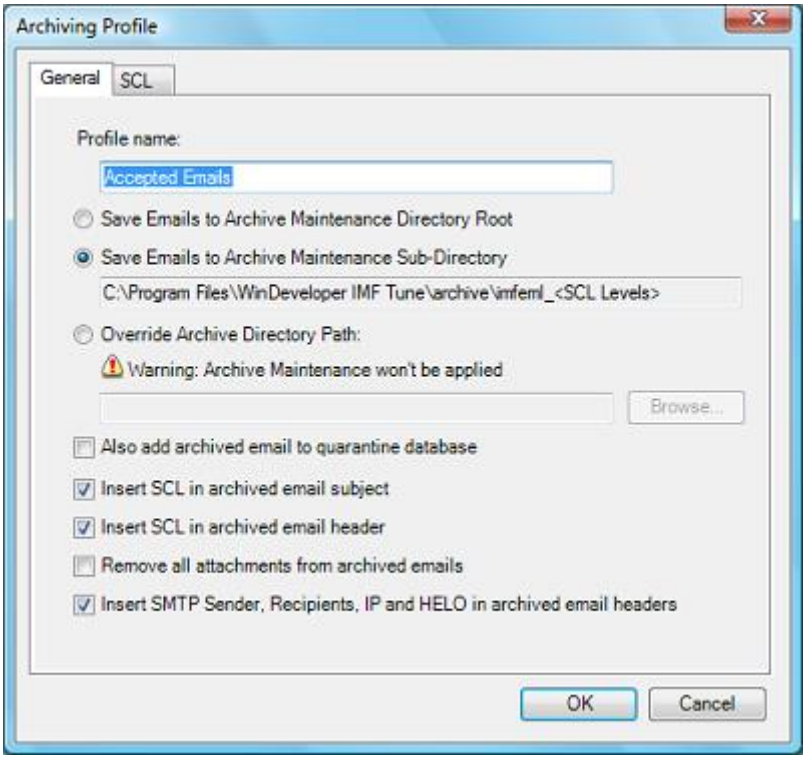
IMF Tune archiving is always available independently of whether the email is accepted, rerouted, deleted or rejected. Thus archiving could be used to keep a simple backup of processed emails or could be used to review emails that were blocked from reaching user mailboxes.

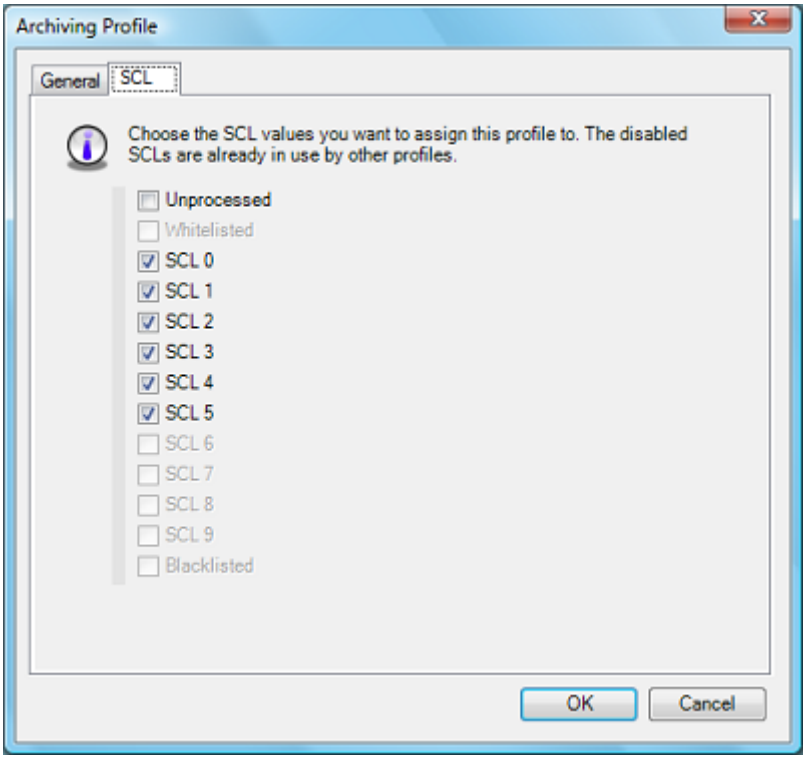
Archiving provides a list interface where each entry groups the settings for a set of SCL ratings. Manipulating the Archiving list simply involves the use of the Add, Remove and Edit buttons.

4.2.1 Archiving Profiles

Archiving options are grouped into Profiles. Each of these includes:

1. Profile Display Name
2. Path to the Archiving directory
3. Publishing the email to a database server
4. Enablement of Additional Email Modifications
5. SCL ratings to which the profile settings are to be applied


Archiving Profile
General
SCL
Profile name:
Accepted Emails
Save Emails to Archive Maintenance Directory Root
Save Emails to Archive Maintenance Sub-Directory
C:\Program Files\WinDeveloper IMF Tune\archive\imfeml_<SCL Levels>
Override Archive Directory Path:
Warning: Archive Maintenance won't be applied
Browse...
Also add archived email to quarantine database
Insert SCL in archived email subject
Insert SCL in archived email header
Remove all attachments from archived emails
Insert SMTP Sender, Recipients, IP and HELO in archived email headers
OK
Cancel


Archiving Profile
General
SCL
Choose the SCL values you want to assign this profile to. The disabled SCLs are already in use by other profiles.
Unprocessed
Whitelisted
SCL 0
SCL 1
SCL 2
SCL 3
SCL 4
SCL 5
SCL 6
SCL 7
SCL 8
SCL 9
Blacklisted
OK
Cancel

4.2.2 Choosing an Archive Directory Path

IMF Tune provides three options for specifying the directory where emails are to be archived. The first two, ‘Save Emails to Archive Maintenance Directory Root’ and ‘Save Emails to Archive Maintenance Sub-Directory’ instruct IMF Tune to compute the path based on the Archive Maintenance configuration. The third option, ‘Override Archive Directory Path’ allows us to specifically set the path to any local disk location.

Archive Maintenance relies on a central disk path configured under the Disk Maintenance | Archives/Quarantine category. These settings are discussed in detail later in this manual. However it is good to appreciate that using Disk Maintenance the configuration of disk paths is centralized.

Consider having multiple archiving profiles. Using Disk Maintenance we avoid specifying an absolute path for each profile. If we later decide to relocate the archive disk location, we simply reconfigure the maintenance root under Disk Maintenance | Archives/Quarantine. IMF Tune would then take care to compute all archive paths relative to the new maintenance root.

If we were to use the ‘Override Archive Directory Path’ option, an absolute path would be required. This leads to setting of paths for each profile. Relocating all archives would thus involve manually editing each profile.

.

4.2.3 Archived Emails Modifications

Archived emails have modification options similar to those available under Email Handling. The difference is that archiving acts on a separate copy of the email. Changes made by Email Handling are visible to the end recipient. Changes made to archived emails are only effective on the copy of the email saved to disk.

Possible archive email modifications include:

- Insert SCL in email subject
- Insert SCL in email headers
- Remove all email attachments
- Insert SMTP Sender, Recipients, IP and EHLO in email headers

The applicability scenarios of these options are very similar to those described for Email Handling. Please refer to the Email Modifications section under Email Handling for more details.

4.2.4 Headers Inserted in Archived Emails

The set of headers that may be inserted into archived emails is very similar to those configurable at the Email Handling category. Nevertheless there is an important difference. Email archiving inserts x-sender and x-receiver headers instead of x-smtp-sender and x-smtp-receiver.

The x-sender and x-smtp-sender end up with the same value i.e. the SMTP FROM originator address. So the change here is purely in the header name. The difference between x-receiver and x-smtp-receiver is more substantial. Whereas x-smtp-receiver is assigned a comma delimited list of recipients, x-receiver holds a single recipient per header. This means that multiple SMTP recipients (RCPT commands) will cause the insertion of multiple x-receiver headers.

The change in the headers makes the IMF Tune archiving 100% compatible with the Exchange pickup/replay email submission mechanism and with the Exchange 2003 IMF archiving functionality. Hence third party applications typically used to manage IMF disk archives may also be used with IMF Tune.

The following table lists the headers that can be inserted into archived emails.

Header	Description
x-scl	The email SCL rating.
x-smtp-ip	The email sender IP.
x-smtp-helo	The SMTP HELO/EHLO host name.
x-sender	The SMTP FROM originator address.
x-receiver	An SMTP RCPT TO recipient address. Multiple SMTP recipients will cause the creation of multiple x-receiver headers.

4.2.5 Publishing Emails to Quarantine

NOTE: A dedicated User Guide for configuring the IMF Tune Quarantine/Reporting functionality is available from the IMF Tune Application Program Group. Please check this document for full details on this topic.

One of the most significant design changes introduced in IMF Tune v5.5 is the shift from email disk archiving to SQL database quarantining. Disk archiving is still 100% backwards compatible. We can easily implement archiving exactly in the same manner as we did in previous releases. However we now have the option to do more by publishing archived emails to a central database server. This is done by selecting the checkbox, at the archive profile configuration:

Also add archived email to quarantine database

If we do not set this checkbox, we have the traditional disk archiving where emails are saved to the specified HDD location. On selecting this option, we instruct IMF Tune to also publish emails to the database server.

Just as in the case of disk archiving, the set of emails to be published to database is controlled from the Archiving profile SCL page. Most typically we will want to publish emails blocked at the server so that we can review these. Thus we select the SCL ratings that are configured for Deletion or Rejection.

Having said that, publishing accepted emails is also possible. One reason why we might want to do this is to analyze the type of emails being assigned midrange SCL ratings, for example SCL4. It is not unusual for us to receive support questions on how to best handle emails assigned such ratings. By publishing these emails, an administrator may gain better understanding of the type of emails falling in this category and thus choose the most appropriate email handling action.

It really is totally up to us. We can choose to only publish emails blocked at the server, but we can also choose to publish emails that were delivered to the user mailboxes.

The Archiving interface immediately highlights the tight coupling that exists between disk archiving and the database server. Indeed **for an email to be published to the database a copy must also be archived to disk**.

The database server is not fed with a full copy of the email. Most notably the database is only supplied with up to 32Kb of body text, no html body content and no file attachments. These potentially large pieces of data are kept at the disk archive.

Let’s see what happens when a user, through the IMF Tune Web interface, releases a quarantined email for delivery. In this case, the IMF Tune server fulfills the request by fetching the email from the disk archive and submits the email for delivery.

4.3 Logging

IMF Tune logging keeps record of processed email in a CSV formatted log file.

The logging information has wide-spread applicability. For example it is always wise to keep a list of all rejected/deleted emails. This gives us the ability to verify which emails were blocked if the necessity arises.

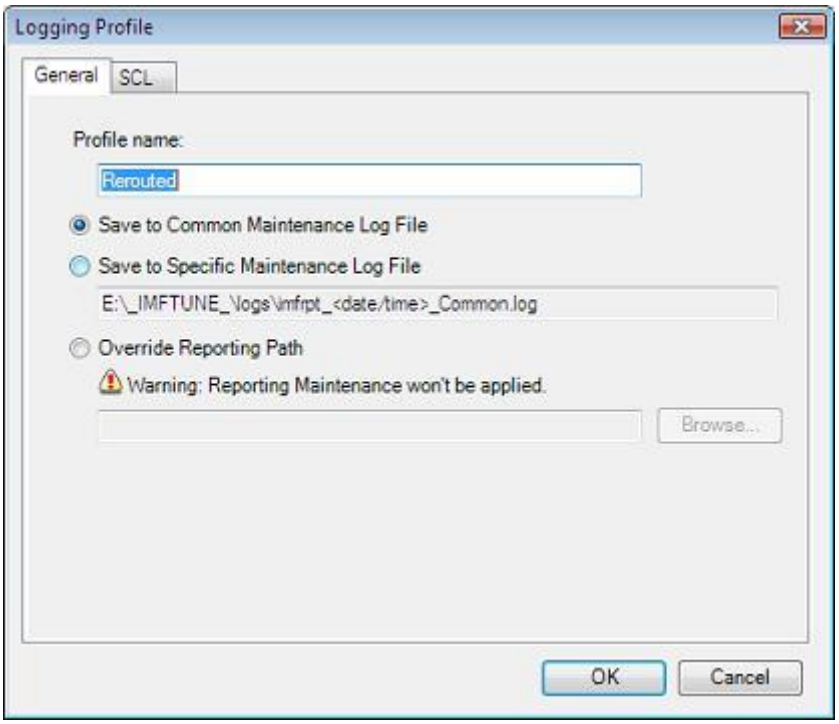
Logged fields such as the remote host IP and the Sender address could be used to populate blacklists. Since the log file is in standard CSV format one could easily open these in MS Excel or MS Access. In this manner we can benefit from the interface and functionality provided by these tools.

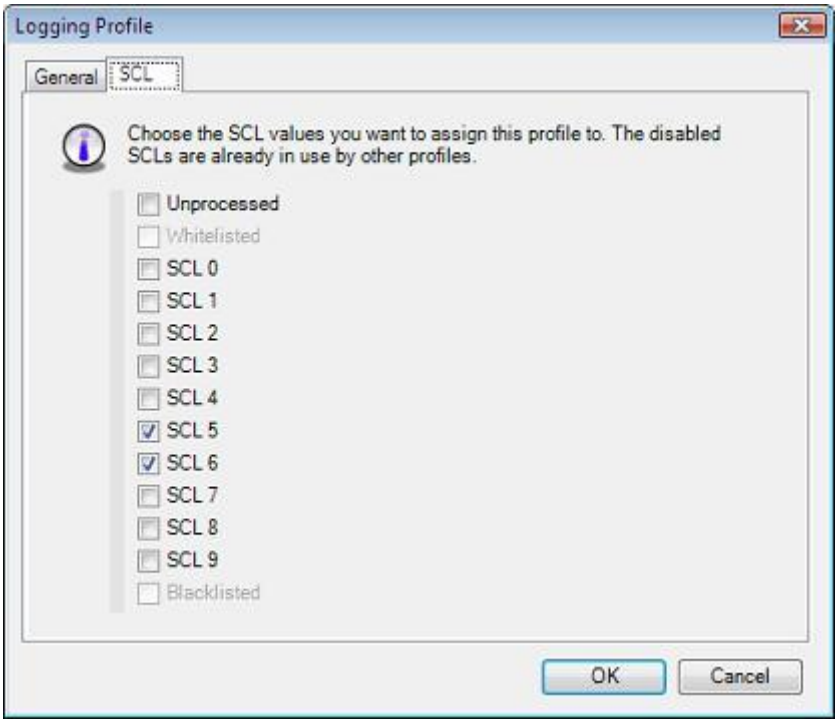
The performance of individual SCL ratings could also be monitored through logging. In this case one could setup different log files for each of the SCL ranges configured at IMF Tune. This will immediately separate the information permitting a more focused analysis. Of course a similar result could be obtained with the help of a database application such as MS Access and the use of SQL queries.

4.3.1 Logging Profiles

Logging options are grouped into Profiles. Each of these includes:

1. Profile Display Name
2. Log file path
3. SCL ratings to which the profile settings are to be applied





The log file path can be identified in one of three ways. The ‘Save to Common Maintenance Log File’ and ‘Save to Specific Maintenance Log File’ options instruct IMF Tune to compute the path based on the Logs/Reports Maintenance configuration. The third option, ‘Override Reporting Path’ allows us to specifically set the path to any local disk location.

Similar to email archiving, IMF Tune provides Disk Maintenance support facilitating the administration of log files. For more details refer to the discussion under Choosing an Archive Directory Path.

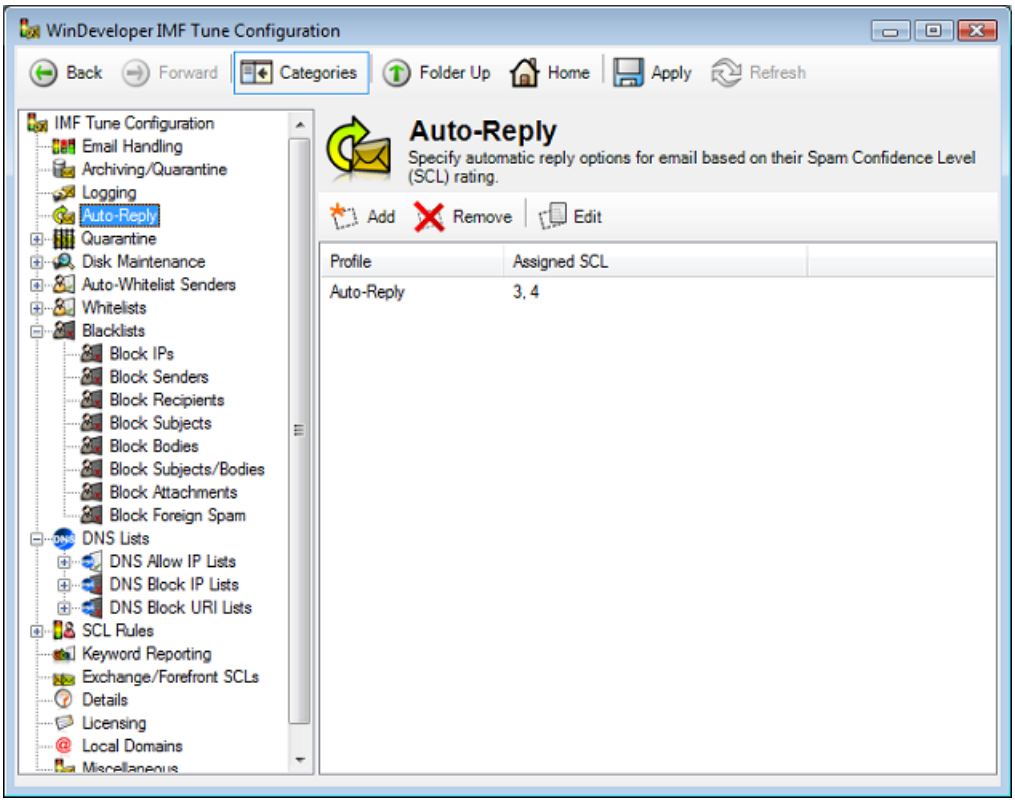
4.3.2 Log File Fields

The following table lists the information logged by IMF Tune:

Field Name	Description
Date	Date when the log entry was created.
Time	Time when the log entry was created.
SCL	The SCL rating assigned to the email.
Subject	The original email subject.
Action	The type of action performed by IMF Tune.
Archive	If enabled the filename of the archived email.
Auto-Reply	If enabled the entry will confirm the successful submission of the auto-reply email.
IP	The email sender IP.
HELO	The SMTP HELO/EHLO host name.
Sender	The SMTP FROM originator address.
Recipients	A comma separated list of SMTP RCPT TO recipient addresses.

4.4 Auto-Replies

Auto-Replies provide the ability to setup an automated response to be sent whenever an email within the configured SCL range is received.



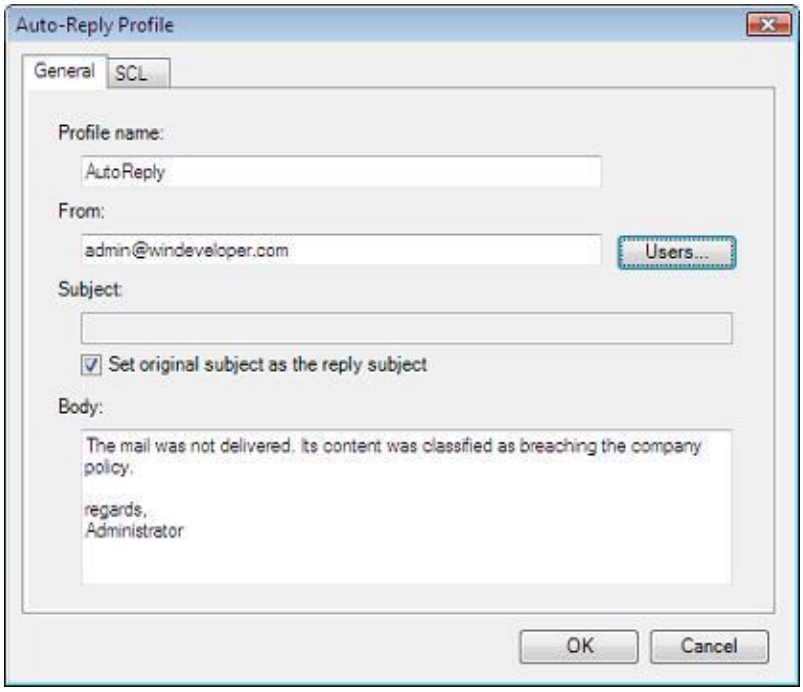
4.4.1 Auto-Reply Profiles

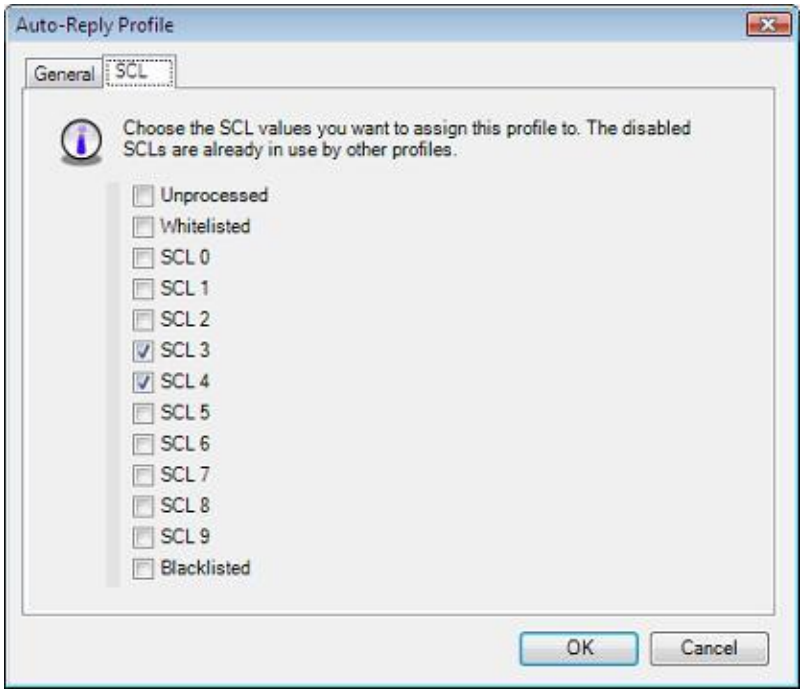
Auto-Reply options are grouped into Profiles. Each of these includes:

1. Profile Display Name

2. Auto-Reply email properties including sender, subject and email body text.

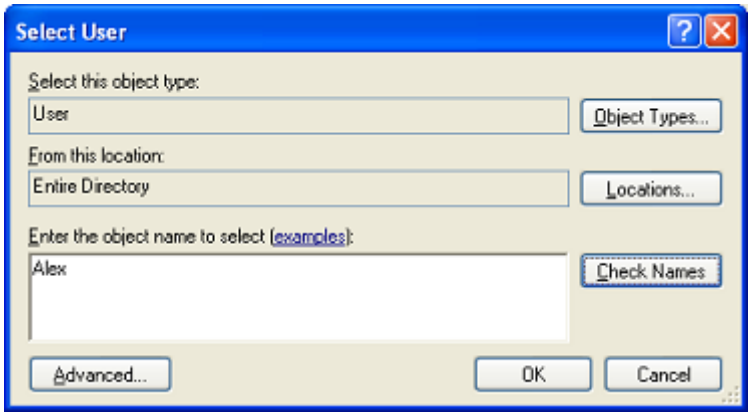
3. SCL ratings to which the profile settings are to be applied





1. At the From edit box specify an SMTP email address. This will be set as the auto-reply sender.

   Alternatively we may select a user from Active Directory by clicking on the Users button.



   In the Select User dialog we may then specify a user name. Clicking on Check Names would then resolve the address. Click OK to close the Select User dialog and set the From address.

2. Next specify the subject of the auto-reply email.

   The Set original subject as the reply subject checkbox instructs IMF Tune to simply set the original subject and prefix it with the standard ‘Re: ’ text.

   Otherwise a fixed subject may be set by clearing the checkbox and entering the text in the Subject edit box.

3. Finally fill in the body text of the auto-reply body.

4.5 Disk Maintenance

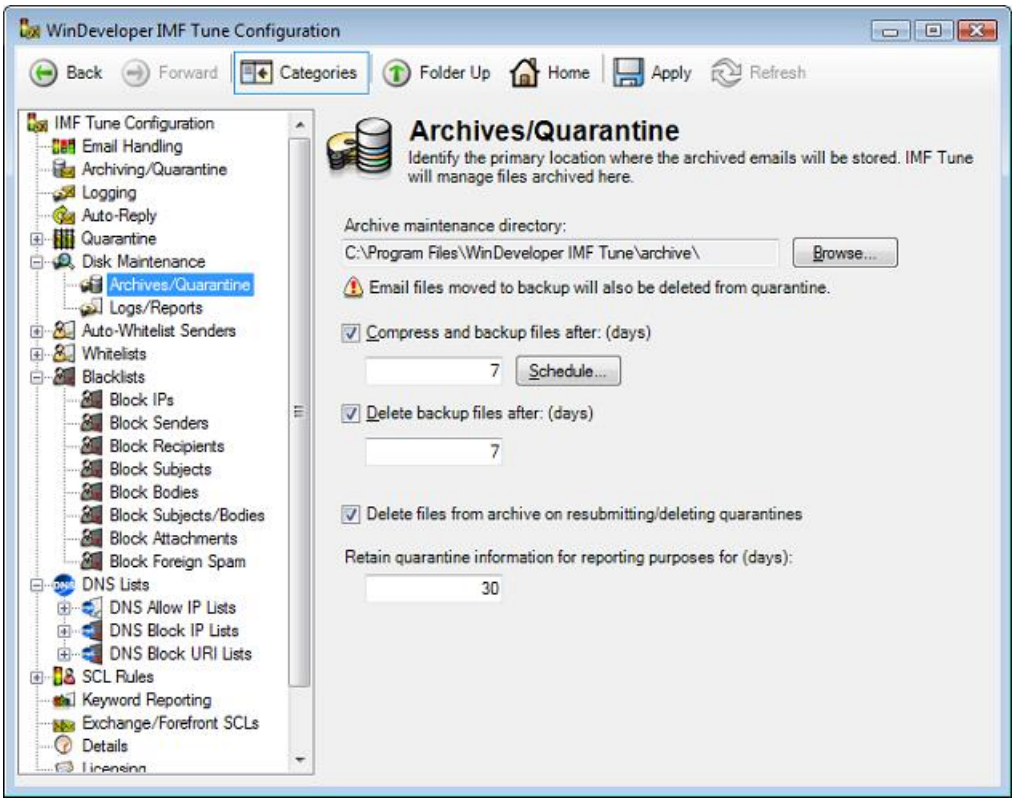
IMF Tune may be configured to archive to disk, quarantine to a database server, and generate CSV reports on all processed emails. If not controlled these operations may exhaust disk space, something that would stop IMF Tune from functioning and potentially affecting other applications running on the same machine. For this reason IMF Tune provides the Disk Maintenance functionality to automate the backup and purging of old email information.

Additionally Disk Maintenance also provides the following benefits:

- Centralized management of all directories used for archiving, logging and reporting.
- A consistent file/directory naming scheme.
- The ability to break logs and reports by date and size.

4.5.1 Archive/Quarantine Maintenance

The core archive/quarantine maintenance settings are available under the Disk Maintenance | Archives/Quarantine category. These comprise the root archive directory path and settings for the backup and deletion of old emails.



This category is really showing settings for the Maintenance of two distinct repositories:

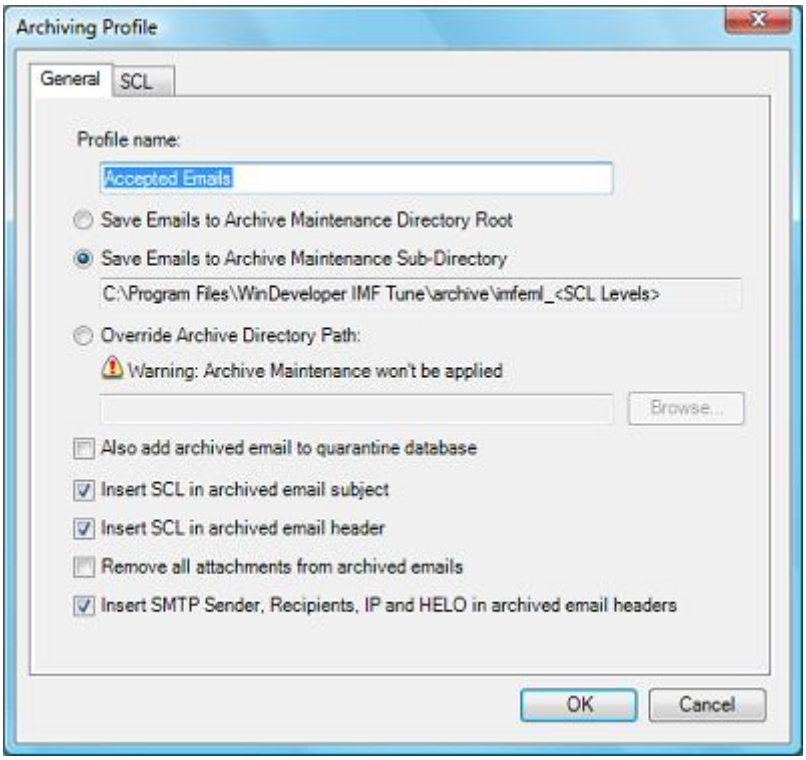
- HDD directories where emails are archived to disk
- Database server where emails are published for moderation/reporting purposes.

We have Maintenance for both of these repositories grouped together because of the tight coupling between the two storages. This was highlighted in Publishing Emails to Quarantine.

4.5.1.1 Archive Maintenance Root

Defining a root archive directory is very beneficial when it comes to managing archiving for different SCL ranges. This point was introduced in the section discussing Email Archiving under Choosing an Archive Directory Path.

Configuring archiving involves creating a profile under the Archiving configuration category:


Archiving Profile
General
SCL
Profile name:
Accepted Emails
Save Emails to Archive Maintenance Directory Root
Save Emails to Archive Maintenance Sub-Directory
C:\Program Files\WinDeveloper IMF Tune\archive\imfeml_<SCL Levels>
Override Archive Directory Path:
Warning: Archive Maintenance won't be applied
Browse...
Also add archived email to quarantine database
Insert SCL in archived email subject
Insert SCL in archived email header
Remove all attachments from archived emails
Insert SMTP Sender, Recipients, IP and HELO in archived email headers
OK
Cancel

Archiving provides three options for specifying the destination directory. The first two are based on Archive Maintenance. Here the destination directory is computed relative to the root configured under Disk Maintenance | Archives/Quarantine. In this manner we can have all archive directories relative to one single root. Thus in case archiving needs to be relocated we just edit a single path.

Archiving Profiles provides the following two options when it comes to disk maintenance based archiving:

Save Emails to Archive Maintenance Directory Root – Emails are simply archived to the maintenance root.

Save Emails to Archive Maintenance Sub-Directory – Emails are archived in a sub-directory to the maintenance root. The sub-directory name is generated based on the SCL range and uses the format:

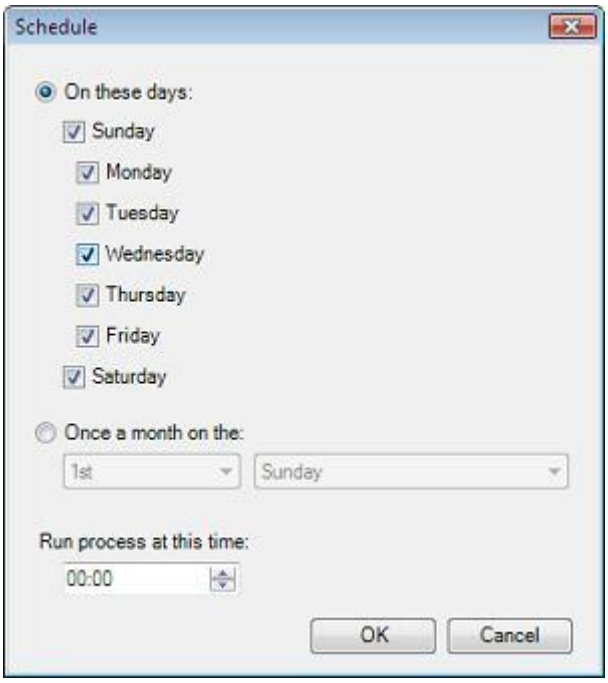
imfeml_a_b_c_.....n – where a, b, c and n are SCL levels configured for this profile.

Using this option the sub-directory is always kept in sync with the SCL range. If the SCL range changes, IMF Tune generates a new sub-directory to which subsequent emails are archived.

4.5.1.2 Disk Archive Backup and Purging

Selecting the ‘Compress & backup files after (days)’ under Archive Maintenance enables the backup functionality. Here we can define the number of days files must age before being backed-up. On running for the first time, a sub-directory named ‘backup’ is created under the maintenance root. Here, batches of emails are saved zip compressed.

Clicking on the schedule button we can choose the days and time when the backup process is triggered.



For daily or weekly backups we choose the 'On these days' schedule option. We can then select the exact days when to run this operation. In cases where the number of files is small we could instead opt for monthly backups by selecting the ‘Once a month’ radio box.

At the bottom of the Schedule dialog ‘Run process at this time’ allow us to provide the exact time when the backup is to start. Although in general the backup operation is not very resource intensive, it is advisable to set a time when the server is not under heavy demand.

Backups will provide more efficient disk usage because of its compression functionality. However files will still continue to accumulate unless these backups are periodically purged. This functionality is enabled by selecting ‘Delete backup files after (days)’. Again here we can specify the number of days the backups must age before purging. This functionality follows the same schedule configured for the backup operation.

4.5.1.3 Quarantine Database Maintenance

NOTE: A dedicated User Guide for configuring the IMF Tune Quarantine/Reporting functionality is available from the IMF Tune Application Program Group. Please check this document for full details on this topic.

The Archives/Quarantine category includes a number of fields specific to the maintenance of the Database server where emails are being published.

At the top of Maintenance | Archives/Quarantine we find a Warning saying:
Email files moved to backup will also be deleted from quarantine.

If the Archive Maintenance option '*Compress and backup files after*' is enabled, emails at the disk archive reaching the specified age limit are moved to backup. At this point, the email may no longer be resubmitted for delivery from the Web Moderator. Thus IMF Tune also deletes the emails from the database server.

At the bottom of Maintenance | Archives/Quarantine category we have a checkbox:
Delete files from archive on resubmitting/deleting quarantines

This option determines whether archived emails should be immediately deleted from disk as soon as these are moderated from the Web interface. Consider a user resubmitting and deleting emails at the moderator. IMF Tune on fulfilling these operations removes the emails from the database. In addition it checks this setting to determine whether or not a copy of the email should be retained on disk.

Retaining emails on disk is useful in a multi-layer backup system where a predictable audit trail is required. You can choose to keep all emails on disk until the archives are backed up and later purged by disk maintenance. This renders the availability of emails archived to disk predictable. If we need to go back and dig some old email from the disk archive, it will still be available.

The last option at the bottom of Maintenance | Archives/Quarantine category is:
Retain quarantine information for reporting purposes for (days)

This is the age limit for email retention at the database server. Emails reaching this limit are purged completely. Note how there is no way to disable this purging and the maximum value here is 999 days.

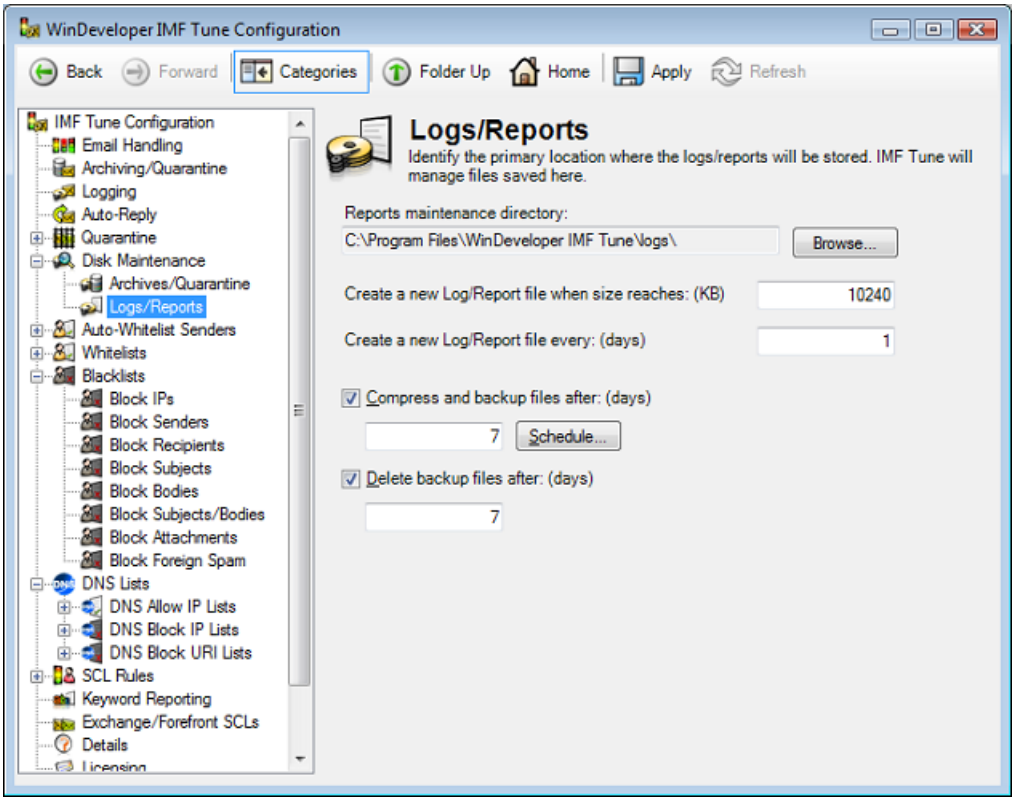
Some might be tempted to employ the IMF Tune database as some kind of permanent email archive. However the Quarantine functionality has not been designed for this purpose. Thus we discourage employing the system in this manner.

The option reads 'Retain quarantine information for reporting purposes' because this age limit determines the number of days reporting information is

retained within the database. In other words the number of days configured here will determine the span of time covered by all reports. As an example let’s say we set this to 30 days. The bar chart showing the number of accepted, rerouted, rejected and deleted emails will show the totals for the last 30 days.

4.5.2 Logs/Reports Maintenance

The Logs/Reports Maintenance functionality is very similar to that for disk archiving. The core maintenance settings are available under the Disk Maintenance | Logs/Reports category. These comprise the root log directory path, settings for breaking files by size and date, and settings for the backup and deletion of old files.



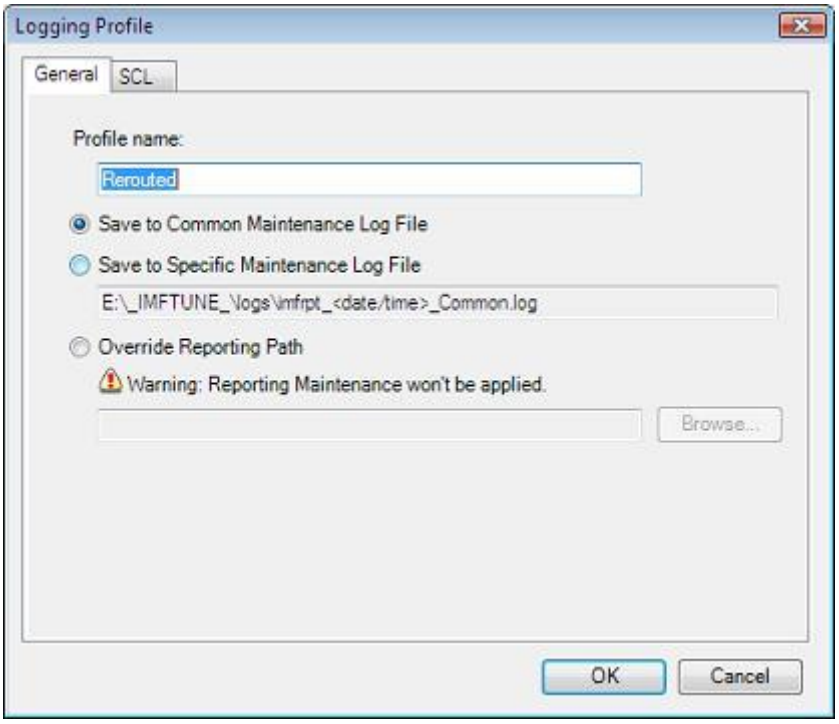
4.5.2.1 Logs/Reports Maintenance Root

Having a root maintenance directory for logs and reports gives the same benefits already discussed for email archiving in Archive Maintenance Root.

The logs/reports maintenance root path works in combination with:

1. Email Logging
2. Keyword Reporting

Configuring email logging involves creating a profile under the Logging configuration category:



The options leveraging disk maintenance here are:

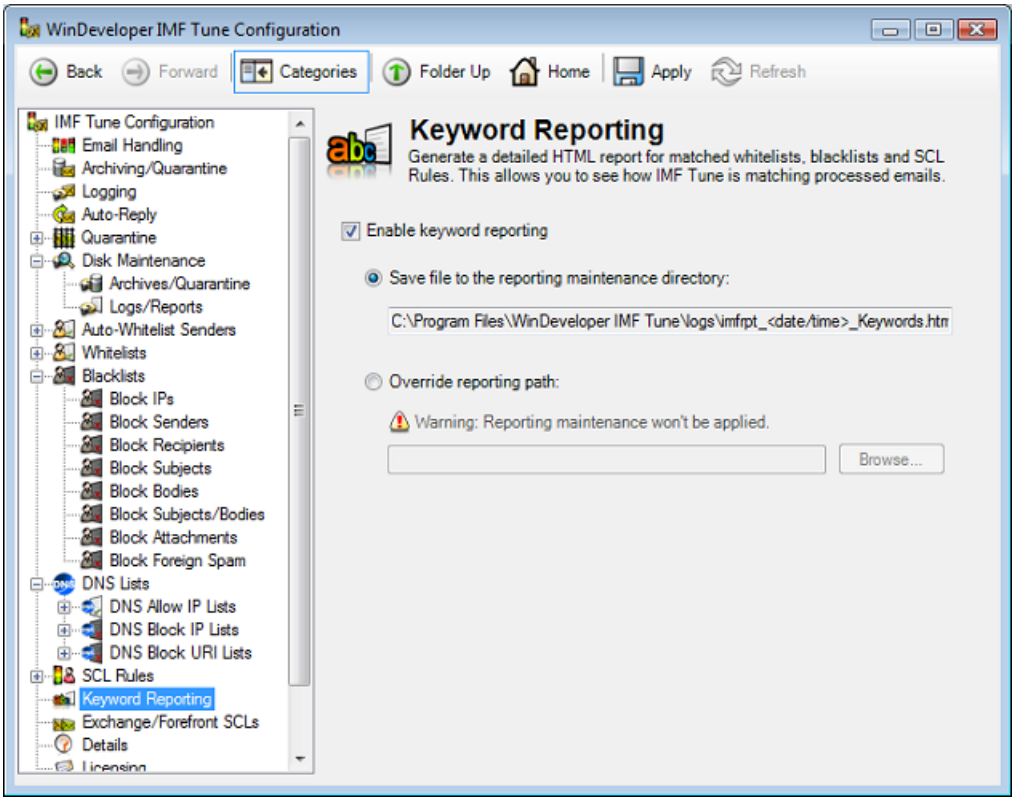
Save to Common Maintenance Log File – Used when logging is to be centralized to a single file. The log file name is automatically generated with the format:

imfrpt_<date/time>_Common.log

Save to Specific Maintenance Log File – Used when logs are to be broken by SCL range. Here the filename is always kept in sync with the SCL range and is named using the following format:

imfrpt_<date/time>_a_b_c....n.log – where a, b, c and n are SCL levels configured for this profile.

Apart for email logging, maintenance is also applied to the Keyword Reporting HTML file.



Keyword reporting only generates a global report file. To enable maintenance the ‘Save to the Reporting Maintenance Directory’ should be selected. The file would then be named using the format:

imfrpt_<date/time>_Keywords.htm

4.5.2.2 Breaking Files by Size and Date

Log and report files are appended whenever an event relevant to their reporting scope occurs. This could lead a single file to grow very large making it more difficult to open and review. For this reason IMF Tune requires the configuration of 2 limits:

1. The maximum file size in KB.

2. The maximum number of days a file can cover.

For performance reasons the size limit cannot be smaller than 1024KB (1MB).

If breaking files by days is preferable, a large size limit can be set so that this is never reached in normal situations. However it is always a good practice to have a size limit (however large) that limits the system in case of unexpected load levels.

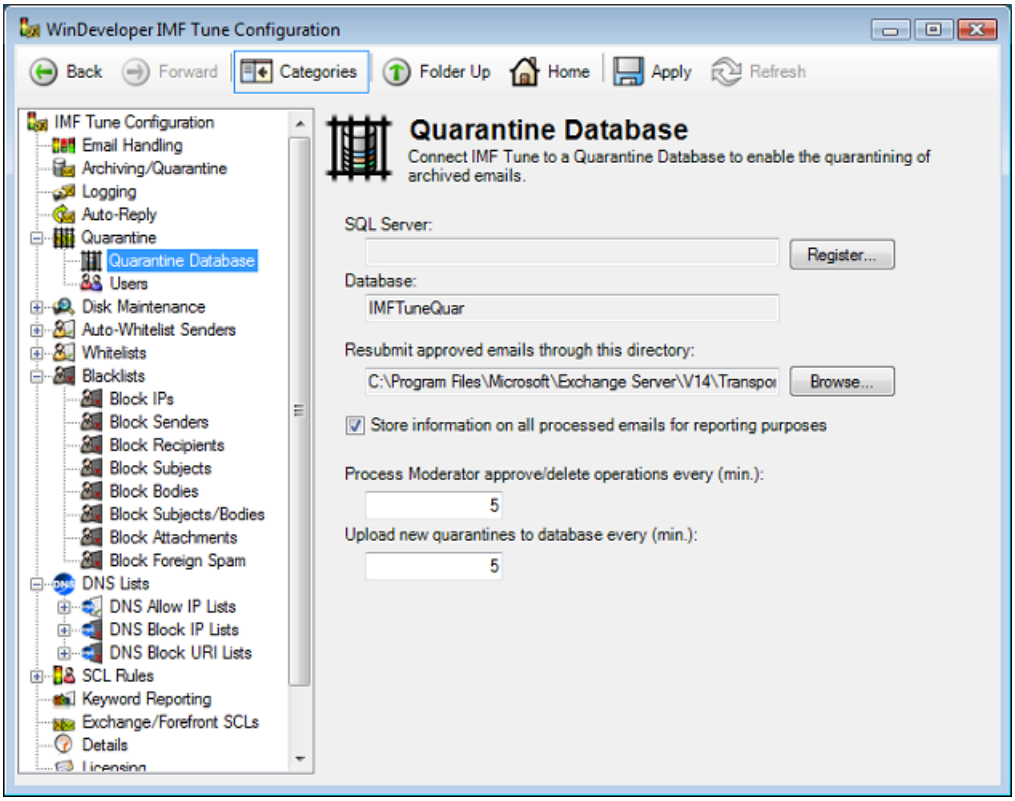
When breaking files by days the starting time is always the beginning of the day i.e. time 00:00.

4.5.2.3 Logs/Reports Backup and Purging

The backup and purging functionality for logs and reports is identical to that for email archives. Again we can set the number of days files are allowed to age before backup and before final deletion. The same schedule interface is also available. For configuration details please refer to Disk Archive Backup and Purging.

4.6 Quarantine

The Quarantine category groups two sub-categories, Quarantine Database and Users.



A dedicated User Guide for configuring the IMF Tune Quarantine/Reporting functionality is available from the IMF Tune Application Program Group. Please check this document for full details on this topic.

4.7 Auto-Whitelist Senders

Sender auto-whitelisting allows the automatic discovery and whitelisting of foreign contacts with whom local users are exchanging emails. Once discovered subsequent emails are automatically whitelisted eliminating the need for manual whitelist configuration.

Within a few days, from enabling auto-whitelisting, a significant number of legitimate emails will be whitelisted bypassing any further filtering. Once the initial discovery is completed, the only legitimate emails undergoing spam filtering will be those from new contacts.

Whitelisting a large proportion of legitimate emails significantly reduces the likeliness of false classification. In turn, this gives us the opportunity to filter spam more aggressively. In other words we are able to lower our filtering thresholds and trap more spam.

Our recommendation is that to let Auto-Whitelisting run for some days. Monitor the number of whitelist hits using Keyword Reporting or even better the ***Moderator/Reporting Web Interface*** (refer to dedicated user guide for details). Both of these allow us to distinguish between Auto-Whitelist hits and Static-Whitelist hits. Once we confirm that many legitimate emails are being auto-whitelisted we can try lowering the SCL blocking threshold at the IMF Tune configuration Email Handling category.

4.7.1 Configuring Sender Auto-Whitelisting

The IMF Tune Sender Auto-Whitelisting configuration offers a lot of control over this functionality.

The checkbox ***Enable Sender Auto-Whitelisting*** activates this functionality.

Limit List to nnnn addresses specifies the maximum number of addresses this list may store.

Remove addresses from the whitelist after nnnn days allows IMF Tune to automatically purge addresses for contacts with whom no emails were exchanged for a long time.

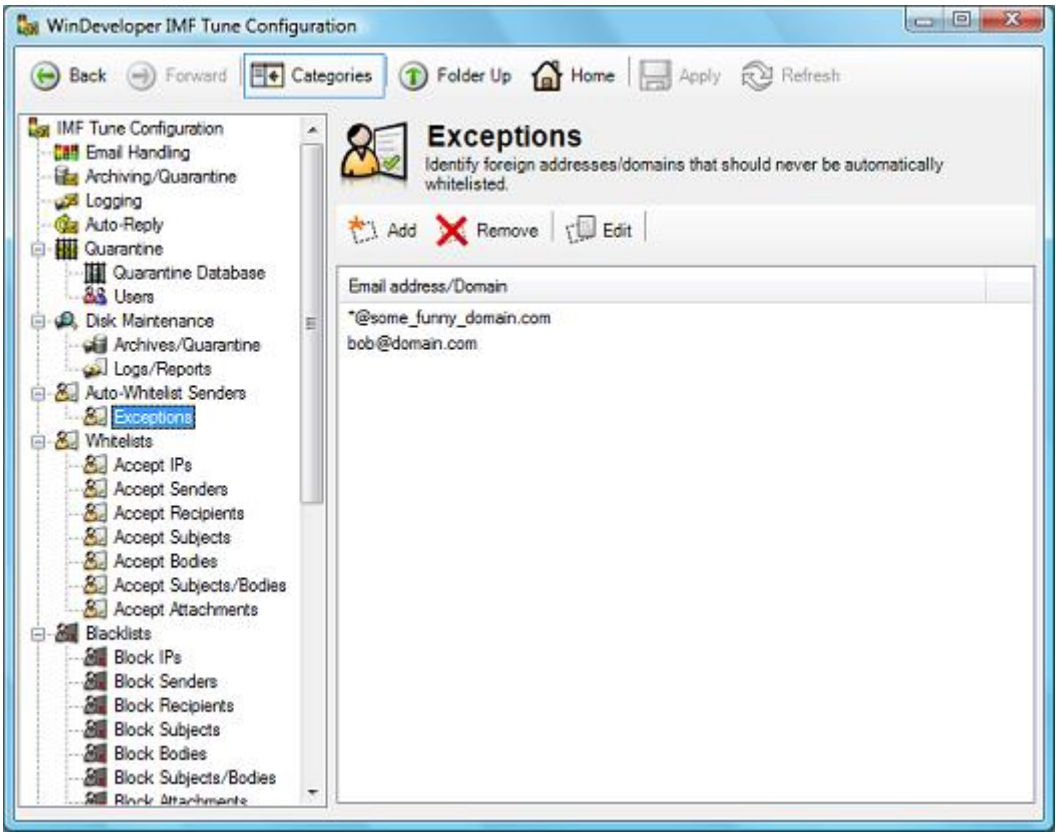
We may choose to whitelist addresses for unlimited time. However in practice very often a contact is only required for a few days, such as the duration of a support incident. Furthermore AWL restarts the day count for an address whenever a new email exchange takes place. In this manner regular contacts are never removed from the list.

Gather foreign addresses from emails sent by, allows us to identify the list of local users whose contacts are to be gathered for whitelisting. We can choose to simply enable this for all users using '***Any local domain user'***. Otherwise we can choose to specify a list of users to exclude or include in the discovery process.

As an example, imagine we have some guest using our email services for a short while. We might not want to whitelist contacts for such guests. As another example, consider the case where we have a mailbox that sends out automated emails to anyone filling some web form. We may choose not to auto-whitelist foreign contacts interacting with this mailbox.

4.7.2 Auto-Whitelist Exceptions

Under the **Auto-Whitelist Senders** category we find the **Exceptions** list.



Here we enter email addresses that IMF Tune should never auto-whitelist. Consider the case where some local user starts an email exchange with a malicious contact, or the case where a contact turns out to be a pest. We can instruct IMF Tune to stop auto-whitelisting an address by entering this to the Exception list.

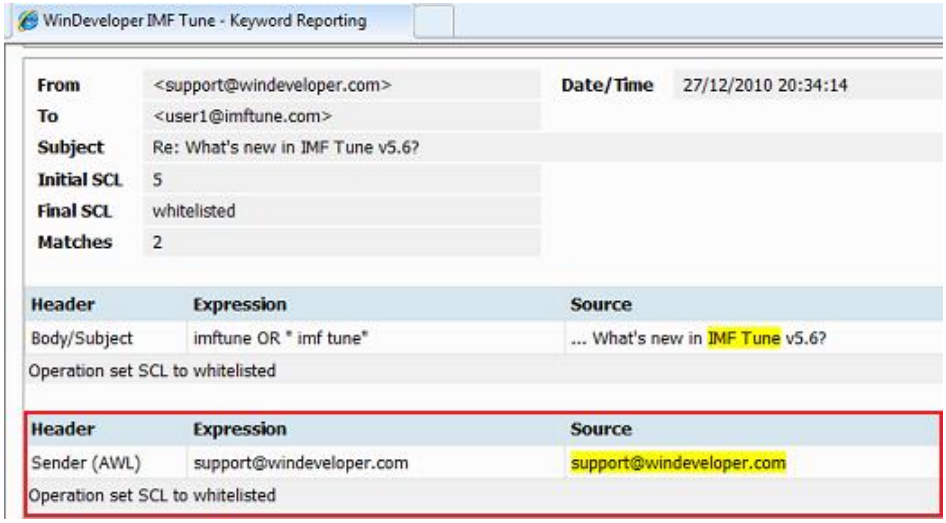
Here we can also enter entire domains using the *@domain format. This instructs IMF Tune not to whitelist any address from that domain. For example users might be using their work mailbox both for business and personal use. Some domains providing personal email addresses might be irrelevant to our Organization business. That's when this list again comes handy.

Note that the Auto-Whitelist Exceptions are not a blacklist. Specifying an address or domain here will only exclude the address from being auto-whitelisted. Emails from these senders will still be processed and might match other static whitelists, blacklists and rules.

4.7.3 Reporting Auto-Whitelist Matches

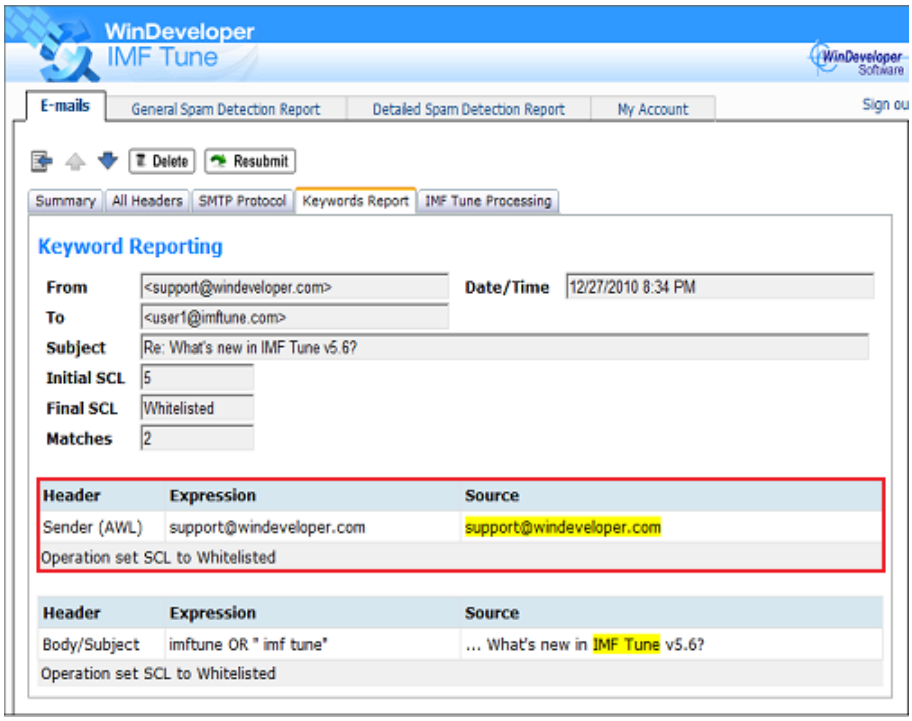
Keyword Reporting and the Moderator/Reporting Web Interface provide special support for Sender Auto-Whitelisting.

This is how a Sender Auto-Whitelist match looks like at the Server HTML Keyword Report:

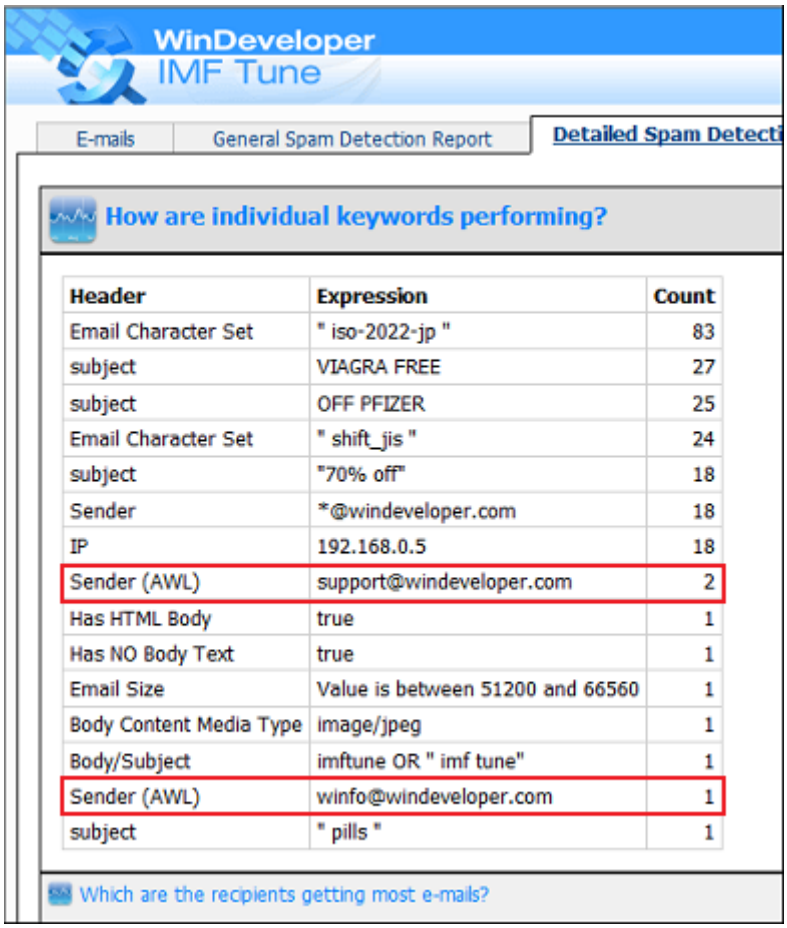


Note how the header name is shown as ***Sender (AWL).***

And this is how the same match is shown at the Moderator/Reporting Web Interface:



The Moderator/Reporting Web Interface will also identify Auto-Whitelist matches at the Keyword Performance report under Detailed Spam Detection Report. Here we can see a couple of addresses being matched:



Header	Expression	Count
Email Character Set	" iso-2022-jp "	83
subject	VIAGRA FREE	27
subject	OFF PFIZER	25
Email Character Set	" shift_jis "	24
subject	"70% off"	18
Sender	*@windeveloper.com	18
IP	192.168.0.5	18
Sender (AWL)	support@windeveloper.com	2
Has HTML Body	true	1
Has NO Body Text	true	1
Email Size	Value is between 51200 and 66560	1
Body Content Media Type	image/jpeg	1
Body/Subject	imftune OR " imf tune"	1
Sender (AWL)	winfo@windeveloper.com	1
subject	" pills "	1

4.7.4 Extracting the List of Auto-Whitelisted Addresses

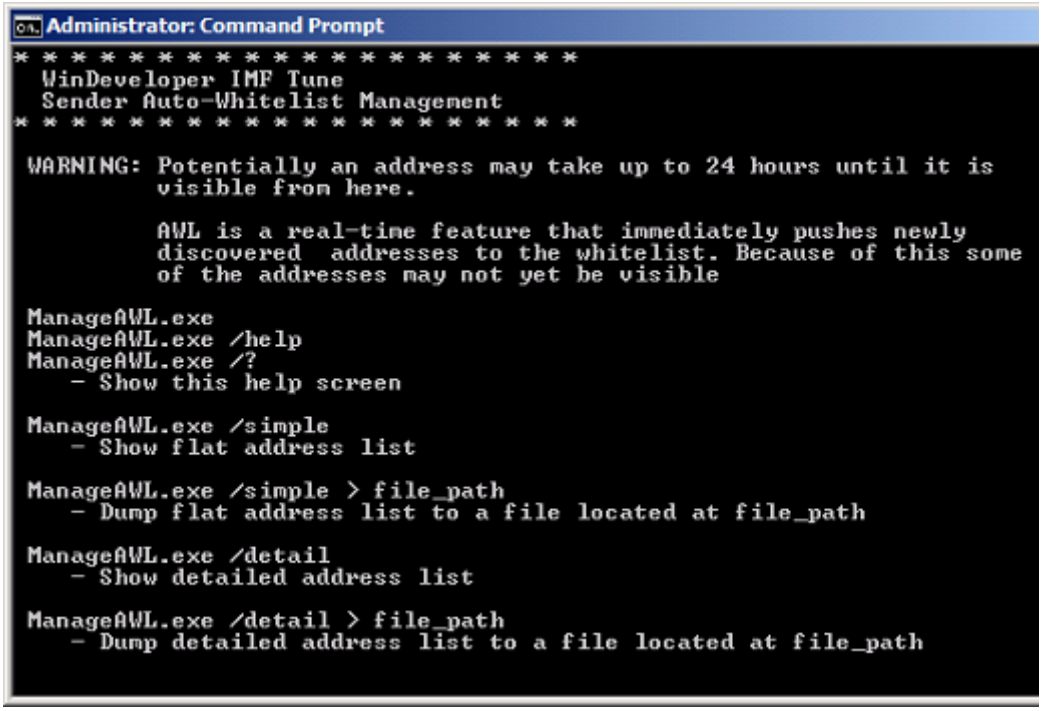
Email addresses gathered at the auto-whitelist (AWL) are not visible from the configuration interface.

ManageAWL is a little command-line tool for extracting the Sender AWL. This tool is available at the IMF Tune application directory. To learn more follow these steps:

1. Open the command prompt
   Important: On platforms supporting User Access Control make sure to open the command prompt using Administrative rights (***Run as Administrator***).

2. Change the directory to the IMF Tune application directory.

3. Run ManageAWL.exe without any parameters to see the usage options.


Administrator: Command Prompt
* *
WinDeveloper IMF Tune
Sender Auto-Whitelist Management
* *
WARNING: Potentially an address may take up to 24 hours until it is visible from here.
AWL is a real-time feature that immediately pushes newly discovered addresses to the whitelist. Because of this some of the addresses may not yet be visible
ManageAWL.exe
ManageAWL.exe /help
ManageAWL.exe /?
- Show this help screen
ManageAWL.exe /simple
- Show flat address list
ManageAWL.exe /simple > file_path
- Dump flat address list to a file located at file_path
ManageAWL.exe /detail
- Show detailed address list
ManageAWL.exe /detail > file_path
- Dump detailed address list to a file located at file_path

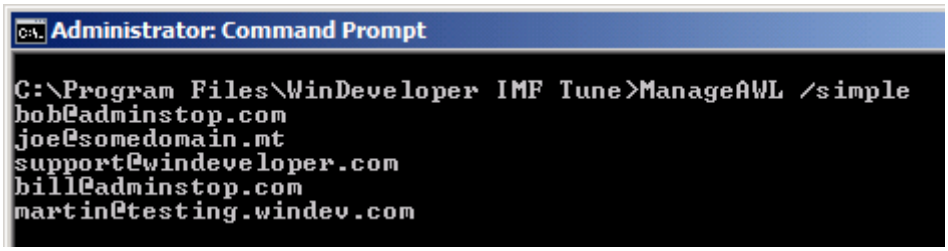
   The tool is very simple; it only requires one of these parameters:
   /Simple – Return a flat list of addresses
   /Detail – Return addresses grouped by date

Important: The help screen alerts us of an important limitation that is worth highlighting. ManageAWL is normally unable to show us the very latest addresses collected by the whitelisting process. Addresses may take up to 24 hours until these become visible. The reason for this has to do with making the process as efficient as possible. IMF Tune immediately starts applying newly discovered addresses for whitelisting; however it only renders the latest

addresses visible in batches. Thus, even though some emails might start being whitelisted, ManageAWL may take some time until it catches up.

4.7.4.1 ManageAWL.exe /Simple

In this mode ManageAWL will produce a flat list of whitelisted addresses:

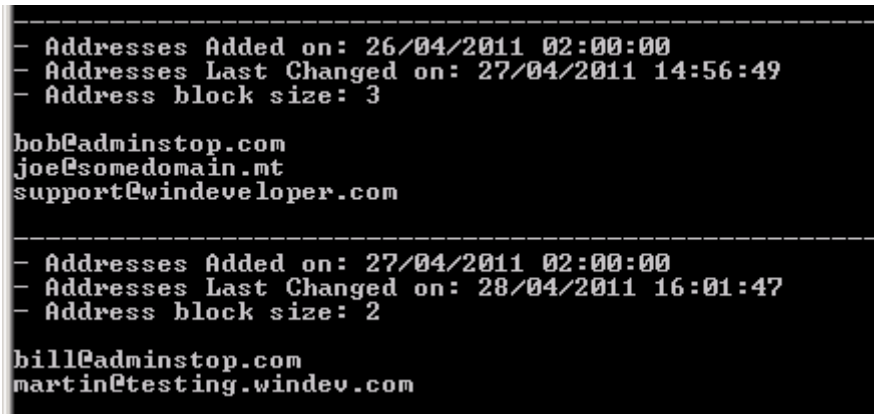


We can choose to dump the list to the command prompt using:
`ManageAWL.exe /simple`

...or else we can redirect the output to a file using:
`ManageAWL.exe /simple > c:\temp\address_list.txt`

4.7.4.2 ManageAWL.exe /Detail

In this mode ManageAWL gives us a better insight of how AWL is working:



Again we can choose between dumping the information to the prompt or to a file:
`ManageAWL.exe /detail`
`ManageAWL.exe /detail > c:\temp\address_list.txt`

Each address batch starts with the header area including:
Addresses Added on
Addresses Last Changed on

The date shown by ‘Addresses Added on’ is used to implement the purging of old addresses. The relevant setting for this is available at the configuration under:
Auto-Whitelist Senders | Remove addresses from the whitelist after

‘Addresses Last Changed on’ is also interesting. IMF Tune moves around addresses each time these are rediscovered. Whenever local users exchange new emails with a foreign contact, the foreign address is removed from the old batch and inserted in the latest address batch. In this manner, contacts with which local users are regularly exchanging emails never get purged.

4.7.4.3 ManageAWL is a Read Only Tool

ManageAWL only gives us read access to the AWL data. It does not allow for deleting addresses. The reason for this is that deleting AWL entries is not all that useful.

Let’ say we have an address we don’t want to whitelist any longer. Removing the address from the AWL will stop IMF Tune from whitelisting it. However this won’t block the AWL process from re-discovering the same address. This is why the correct solution is to add any such addresses to the AWL Exception list under:
Auto-Whitelist Senders | Exceptions

When adding an exception, IMF Tune will:

1. Stop whitelisting the address
2. Learn not to whitelist it again in the future

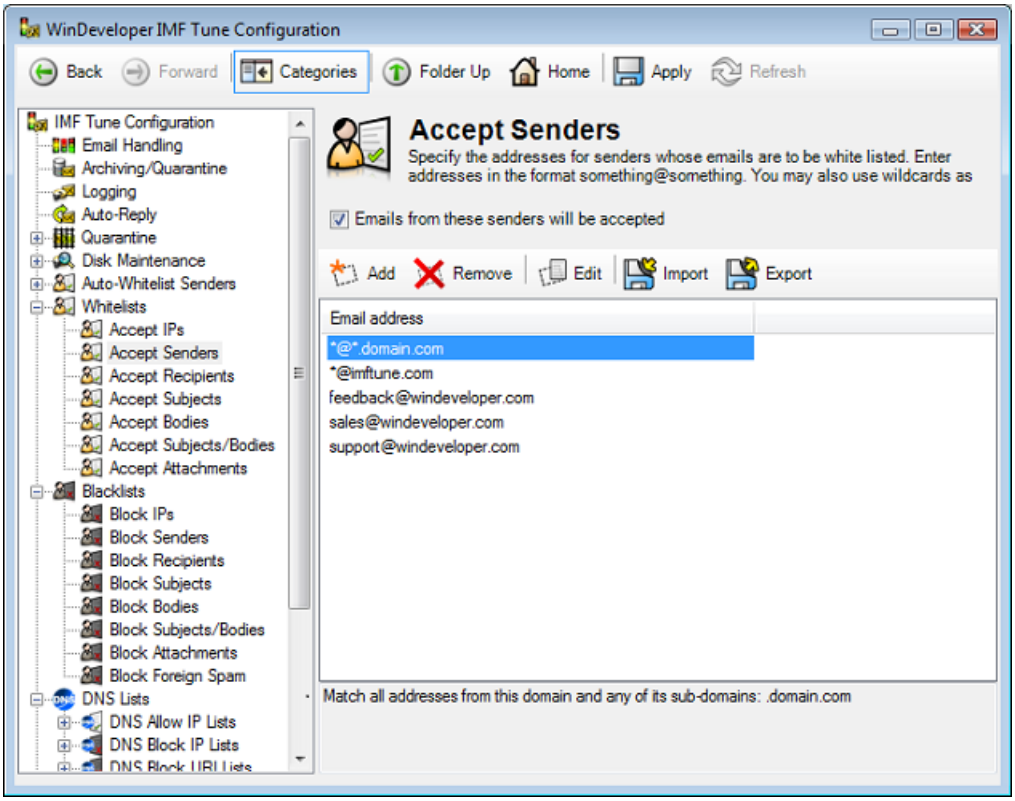
4.8 Working with Whitelists

Whitelisting enables identifying legitimate emails. Through it, emails avoid the risk of being misclassified as spam. On whitelisting any previously assigned SCL rating is overridden. Thus, this classification takes priority over SCLs assigned by IMF and by the IMF Tune Blacklisting and SCL Rules.

The Whitelists category groups IP, Sender, Recipient, Subject, Body, combined Subject/Body, and Attachment whitelisting.

4.8.1 Accept Senders and Accept Recipients Lists

The Accept Senders and Accept Recipients categories enable the whitelisting of email addresses and domains. IMF Tune attempts to match SMTP addresses against these lists. If a match is found the email is whitelisted.

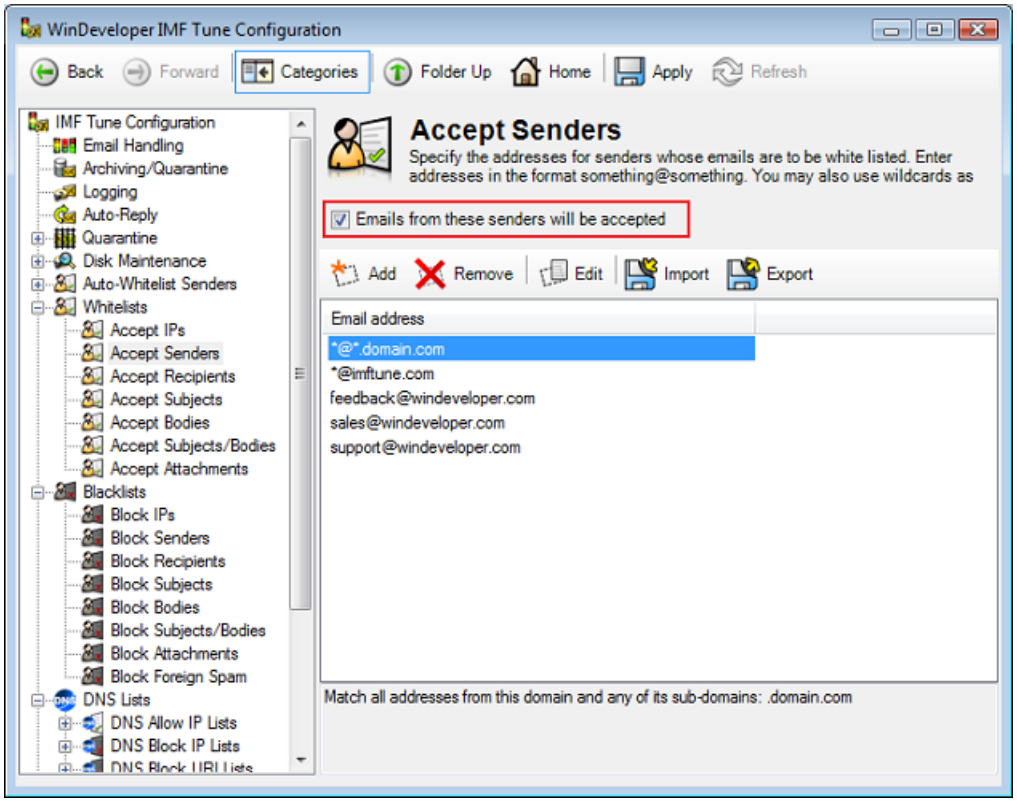


Note that for a single email, the sender address may be identified in a number of ways. IMF Tune checks all of these locations:

- SMTP MAIL FROM address
- From header
- Sender header
- Resent-From header
- Resent-Sender header

4.8.1.1 Working with Address Lists

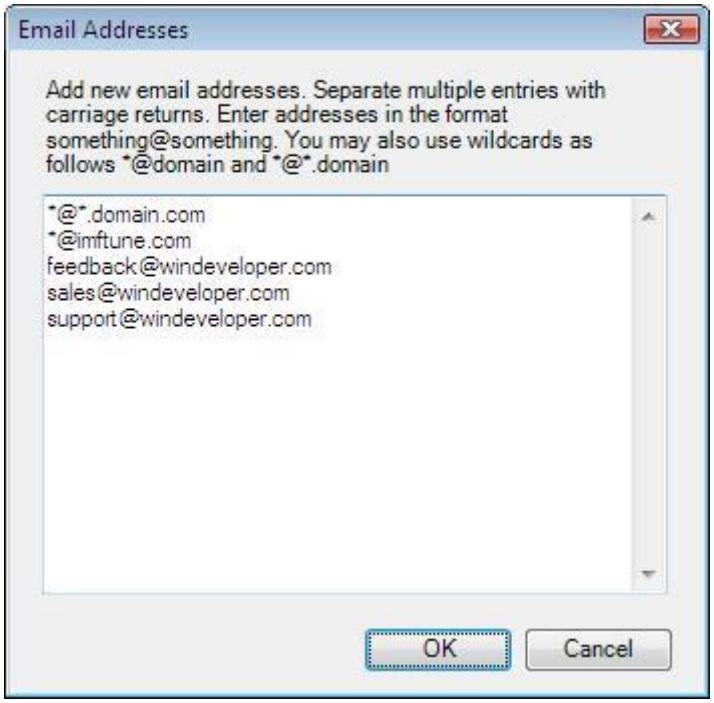
To enable/disable an address list set/clear the checkbox at the top. Setting the checkbox will activate the list and IMF Tune will process the addresses against incoming emails.



Next we can add, remove and edit email addresses using the buttons at the top. Everything is fairly intuitive. We just need to be aware of how to use wildcards. This is discussed in the section that follows ***Adding New Addresses***.

4.8.1.2 Adding New Addresses

To add new addresses click on the Add button. A dialog opens where multiple email addresses may be entered:



Enter each address in a separate line by hitting the carriage return key. The list can handle up to 64Kb of data at a time. To enter more addresses click OK to save and close the dialog. Next click Add again to re-open the dialog and enter more addresses. Otherwise we may use the address list import functionality to quickly add large lists of addresses.

We may include all email addresses for a specific domain by using the * wildcard. The following wildcard formats are supported:
***@<domain>**
***@*.<domain>**

4.8.1.3 Importing Email Addresses

IMF Tune enables the insertion of addresses into white/black lists through the import functionality. For the import to work the source file must meet the following requirements:

1. Importing only supports plain text files. The file may be encoded in 7-bit ASCII, UTF-8 or UTF-16. Although two UTF encoding formats are supported, all characters are expected to be within the standard Windows 1252 character set.

2. Multiple address entries must be separated by a carriage return line feed (CRLF) sequence. For files generated on non-Windows platforms the line feed only separator (LF) is also supported.

In order to see a sample of a correctly formatted file use the Export functionality.

The import process includes a validation procedure that could reject some of the entries being imported. For example if an address contains illegal wildcards that entry would be rejected.

When importing a large number of addresses it may be difficult to determine which addresses failed to be imported. For this reason, whenever importing, the ImportReport.log file will be generated. This file is located in the main IMF Tune program directory and is overwritten on each import. The log file will show how each of the imported entries was handled and whether or not the entry was rejected due to validation reasons.

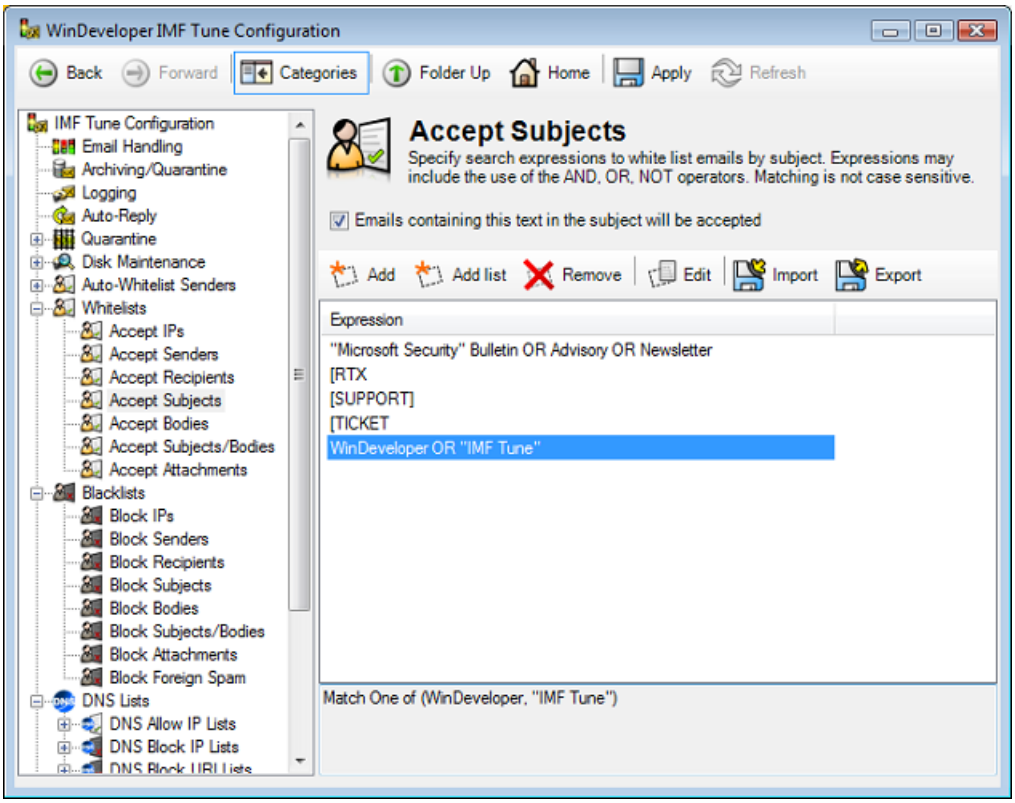
4.8.1.4 Exporting Email Addresses

IMF Tune also supports exporting address lists to an external text file. The export is correctly formatted to the IMF Tune import specifications. Thus we may use the export and import functionality in order to quickly replicate configurations on multiple IMF Tune installs.

Exports are always encoded in UTF-8. For details on the format of the exported file refer to Importing Email Addresses.

4.8.2 Accept Subjects and Accept Bodies Lists

The Accept Subjects, Accept Bodies and Accept Subjects/Bodies categories enable the whitelisting of emails based on the email subject and body text. IMF Tune attempts to match the subject and body against keywords within these lists. If a match is found the email is whitelisted.



As the name of the lists imply the Accept Subjects list is applied against the email subject, whereas the Accept Bodies is enforced against the email text and html bodies.

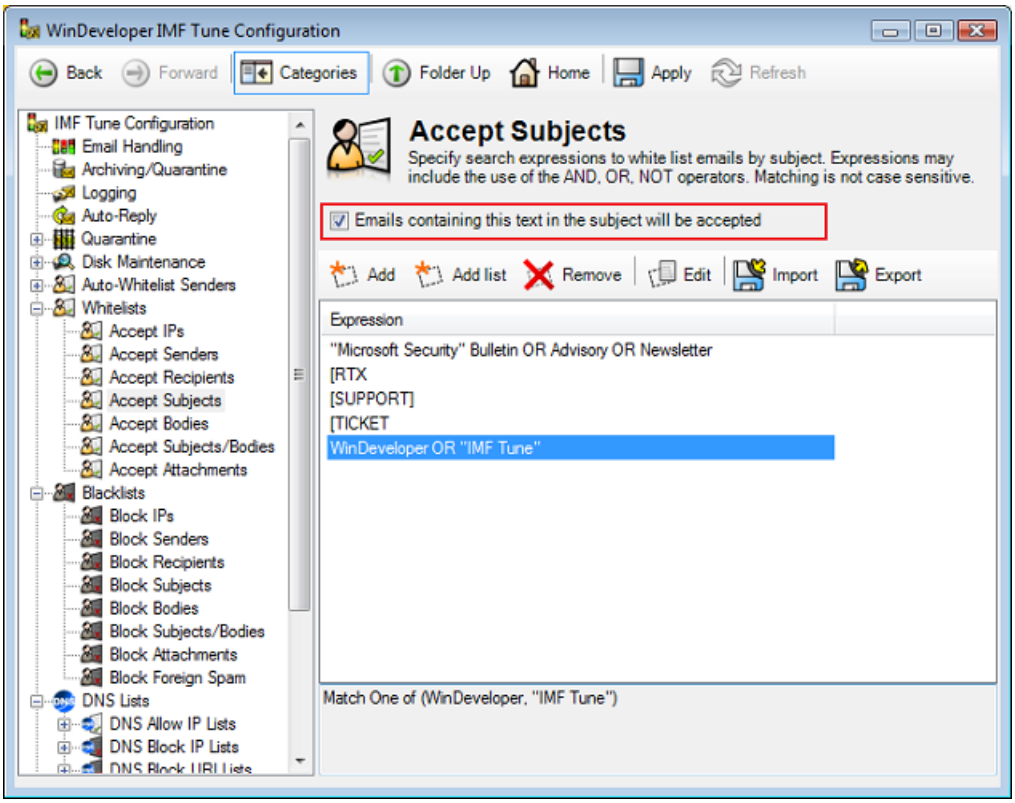
The Accept Subjects/Bodies list is applied against the combined email subject and body information. The keywords are searched against both of them. This saves us from entering the same keywords in both Subject and Body lists when the exact keyword location is not relevant. Note that when an expression is composed of multiple keywords it is possible that one keyword is matched at the subject and another is matched at the body.

These lists support fairly advanced keyword expressions. The operators AND, OR, NOT may be used to combine multiple keywords into a single expression. Double quotes may also be used to enforce exact matching. For more details check the section Constructing Search Expressions.

The SCL Rules configuration also provides the ability to whitelist emails by subject and body. Additionally SCL Rules provide more control over email processing.

4.8.2.1 Working with Keyword Lists

To enable/disable any of the keyword lists set/clear the checkbox at the top. Setting the checkbox will activate the list and IMF Tune will process the keywords against incoming emails.

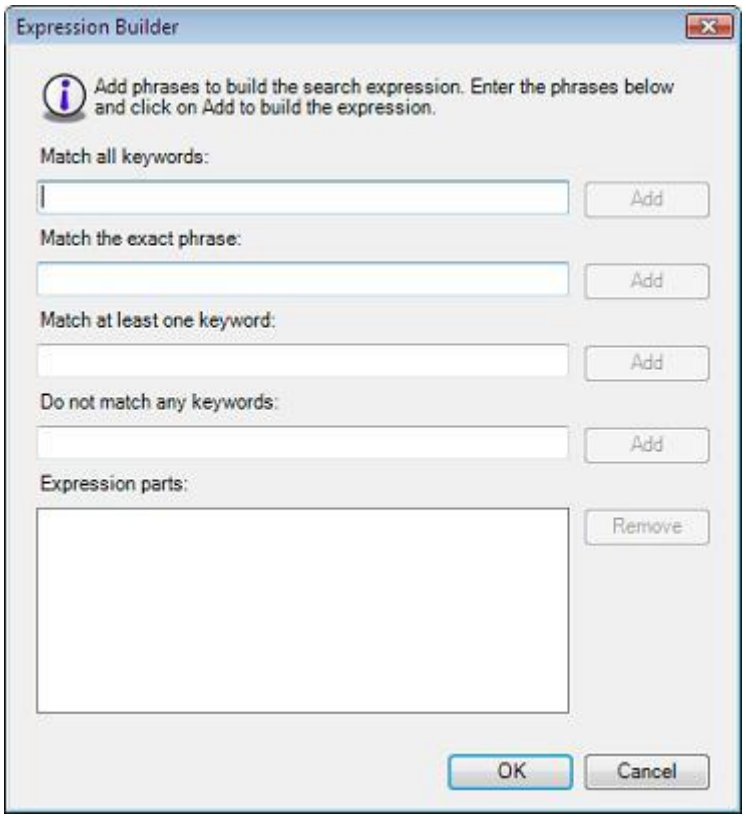


Next we can add, remove and edit keyword expressions using the buttons at the top.

4.8.2.2 Adding a New Keyword Expression

IMF Tune provides two interfaces for adding new keyword expressions, the Expression Builder and the Add List interface. The Expression Builder offers a simple interface to easily construct complex keyword expressions. It helps with correctly using the AND, OR, NOT operators and with double quoting phrases when necessary.

Click on the Add button at one of the Subject, Body, Subject/Body keyword lists to open the Expression Builder dialog:



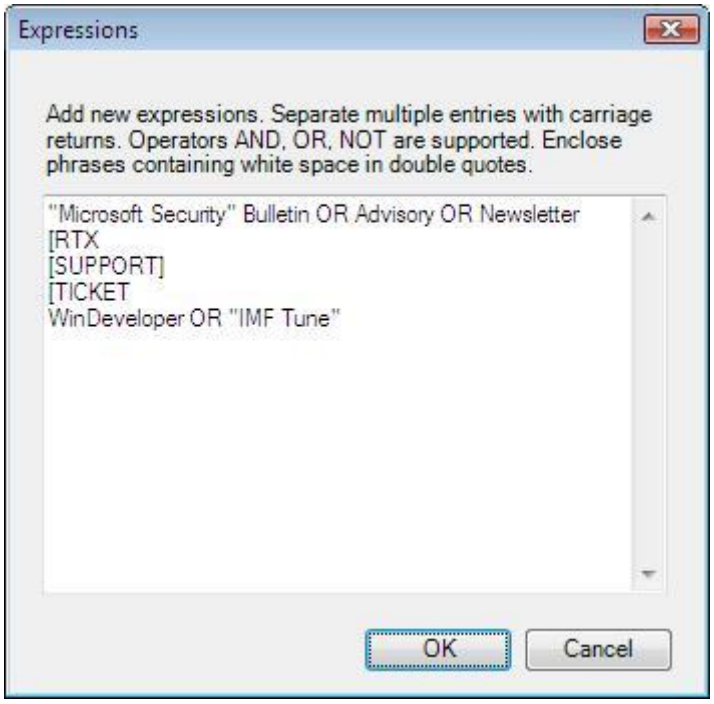
We may now construct the expressions by inserting different types of keywords and phrases. Fill in any of the four edit boxes and click on the adjacent Add button. This will insert each of the sub-expressions into the Expression Parts list at the bottom. When done, click OK to add the new expression. For more details on how to use this interface check the section Working with the Expression Builder.

4.8.2.3 Adding a List of Keyword Expressions

IMF Tune provides two interfaces for adding new keyword expressions, the Expression Builder and the Add List interface.

The Add List interface provides a simple interface through which multiple expressions may easily be entered. Nevertheless it does not provide assistance with using the AND, OR, NOT operators. Thus constructing more complex expressions requires understanding the expression syntax rules. Check the Constructing Search Expressions section for details on expression syntax.

Click on the Add List button at one of the Subject, Body, Subject/Body keyword lists to open the expression list dialog:

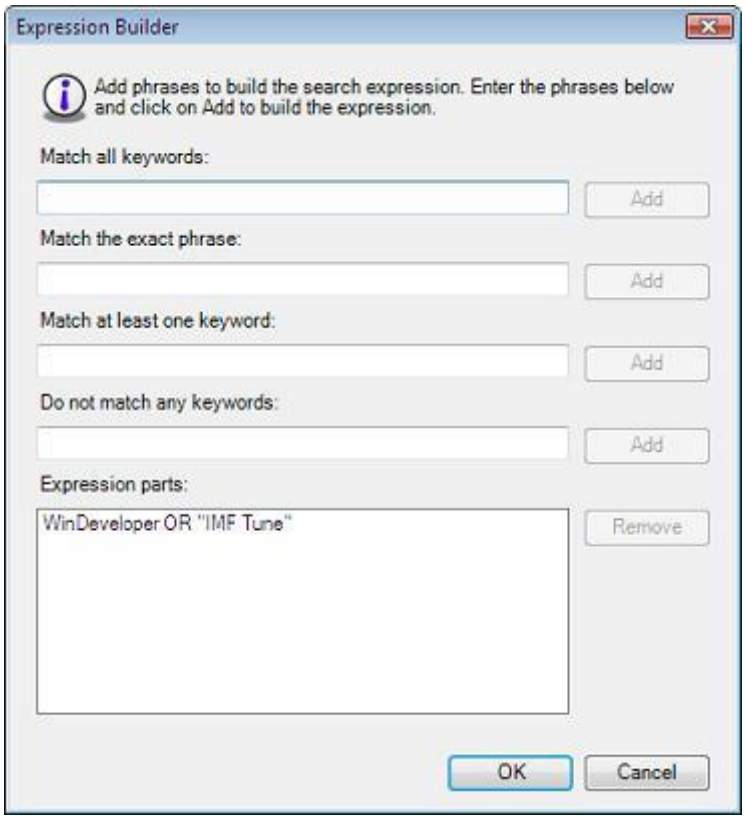

Expressions
Add new expressions. Separate multiple entries with carriage returns. Operators AND, OR, NOT are supported. Enclose phrases containing white space in double quotes.
"Microsoft Security" Bulletin OR Advisory OR Newsletter
[RTX
[SUPPORT]
[TICKET
WinDeveloper OR "IMF Tune"
OK
Cancel

Enter each expression in a separate line by hitting the carriage return key. The list can handle up to 64Kb of data at a time. To enter more keywords click OK to save and close the dialog. Next click Add List again to re-open the dialog and enter more keywords. Otherwise we may use the keyword list import functionality to quickly add large lists of expressions.

Expressions here may also include the AND, OR, NOT operators and the use of double quotes. The list interface will automatically validate each of the expressions on clicking OK and notify us of any invalid expressions.

4.8.2.4 Editing Existing Keywords

IMF Tune supports editing expressions through the Expression Builder interface. Double click the expression, or select the expression and click on the Edit button.



To delete any expression part, select this from the Expression Parts list and click on the Remove button. Likewise we may add keywords by filling the appropriate edit box and clicking the corresponding Add button. When done, click OK to save changes. For more details on using the Expression Builder check Working with the Expression Builder.

4.8.2.5 Importing Keyword Expressions

IMF Tune enables the insertion of keyword expressions into white/black lists through the import functionality. For the import to work the source file must meet the following requirements:

1. Importing only supports plain text files. The file may be encoded in 7-bit ASCII, UTF-8 or UTF-16. Although two UTF encoding formats are supported, all characters are expected to be within the standard Windows 1252 character set.

2. Multiple keyword expressions must be separated by a carriage return line feed (CRLF) sequence. For files generated on non-Windows platforms the line feed only separator (LF) is also supported.

In order to see a sample of a correctly formatted file use the Export functionality.

The import process includes a validation procedure that could reject some of the entries being imported. For example if an expression contains illegal use of the AND, OR, NOT operators that entry would not be imported.

When importing a large number of expressions it may be difficult to determine which expressions failed to be imported. For this reason, whenever importing, the ImportReport.log file will be generated. This file is located in the main IMF Tune program directory and is overwritten on each import. The log file will show how each of the imported entries was handled and whether or not the entry was rejected due to validation reasons.

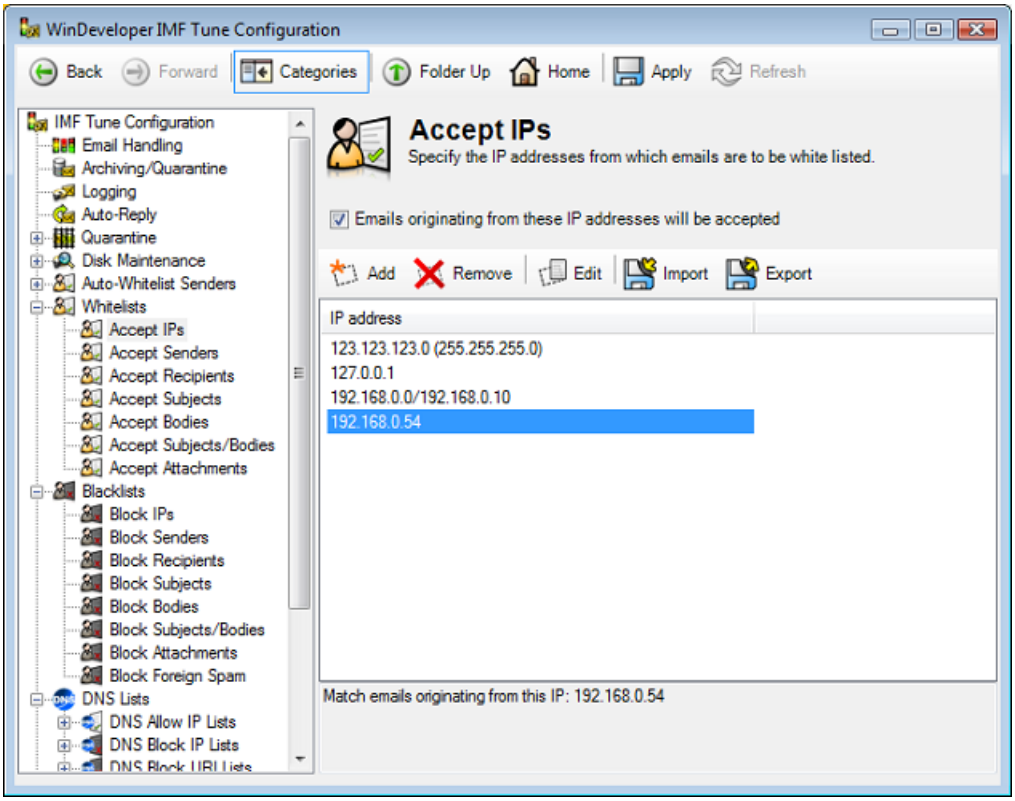
4.8.2.6 Exporting Keyword Expressions

IMF Tune also supports exporting expression lists to an external text file. The export is correctly formatted to the IMF Tune import specifications. Thus we may use the export and import functionality in order to quickly replicate configurations on multiple IMF Tune installs.

Exports are always encoded in UTF-8. For details on the format of the exported file refer to Importing Keyword Expressions.

4.8.3 Accept IPs

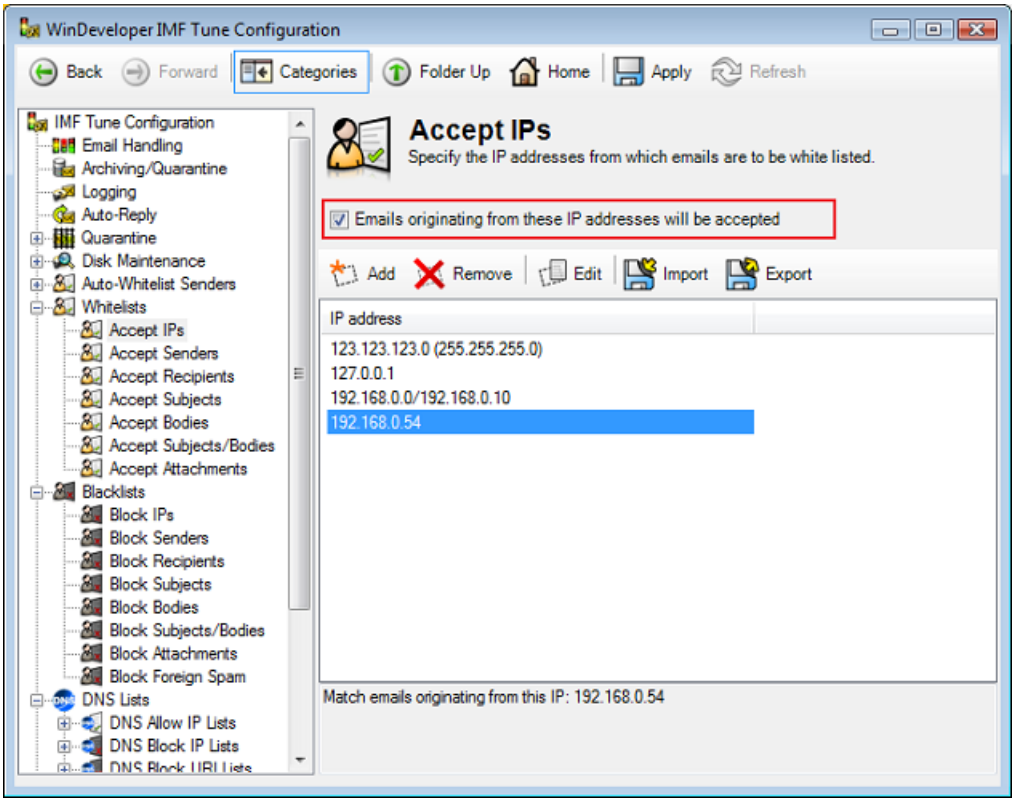
The Accept IPs category enables the whitelisting of emails based on the originating host IP.



The IP list can be fed with single IPs, IP ranges and IP/Mask pairs.

4.8.3.1 Working with the IP Lists

To enable/disable the IP lists set/clear the checkbox at the top. Setting the checkbox will activate the list and IMF Tune will process the IPs against incoming emails.



Next we can add, remove and edit IP entries using the buttons at the top of the list.

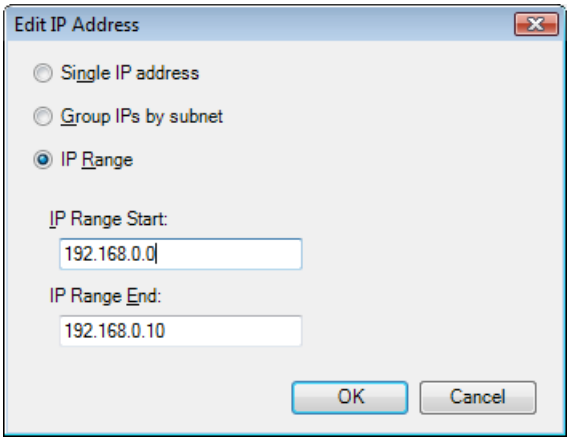
4.8.3.2 Adding/Editing IP Entries

IMF Tune allows the entry of single IPs, IP ranges and IP/Mask pairs.

In an IP range we specify the lower and upper IP limits. IMF Tune would then match all IPs between these two limits.

An IP/Mask pair also identifies a set of IPs. This time the relevant IPs are determined by combining the IP and Mask as in subnetting.

Click on the Add button to open the IP configuration dialog:



From here select *Single IP address*, *Group IPs by subnet* or *IP Range*. Next we fill the edit boxes that follow with the IPv4 values to be matched.

To edit an IP entry, select this from the whitelist and click on the Edit button.

4.8.3.3 Importing IPs

IMF Tune enables the insertion of IPs into white/black lists through the import functionality. For the import to work the source file must meet the following requirements:

1. Importing only supports plain text files. The file may be encoded in 7-bit ASCII, UTF-8 or UTF-16.

2. Multiple IP entries must be separated by a carriage return line feed (CRLF) sequence. For files generated on non-Windows platforms the line feed only separator (LF) is also supported.

3. Single IP entries must be in the format:
   xxx.xxx.xxx.xxx.

4. IP/Mask pairs must be in the format:
   xxx.xxx.xxx.xxx (mmm.mmm.mmm.mmm)

   Here the mask portion is enclosed in brackets.

5. IP Ranges must be in the format:
   xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy

   xxx.xxx.xxx.xxx is the lower IP limit
   yyy.yyy.yyy.yyy is the upper IP limit

In the same file we can have a mix of single IPs, IP/Mask pairs and IP Ranges. We just need to follow the above formatting rules.

To see a sample of a correctly formatted file use the Export functionality.

The import process includes a validation procedure that could reject some of the entries being imported. For example if an IP does not match the required formats that entry would not be imported.

When importing a large number of IPs it may be difficult to determine which IPs failed to be imported. For this reason, whenever importing, the ImportReport.log file will be generated. This file is located in the main IMF Tune program directory and is overwritten on each import. The log file will show how each of the imported entries was handled and whether or not the entry was rejected due to validation reasons.

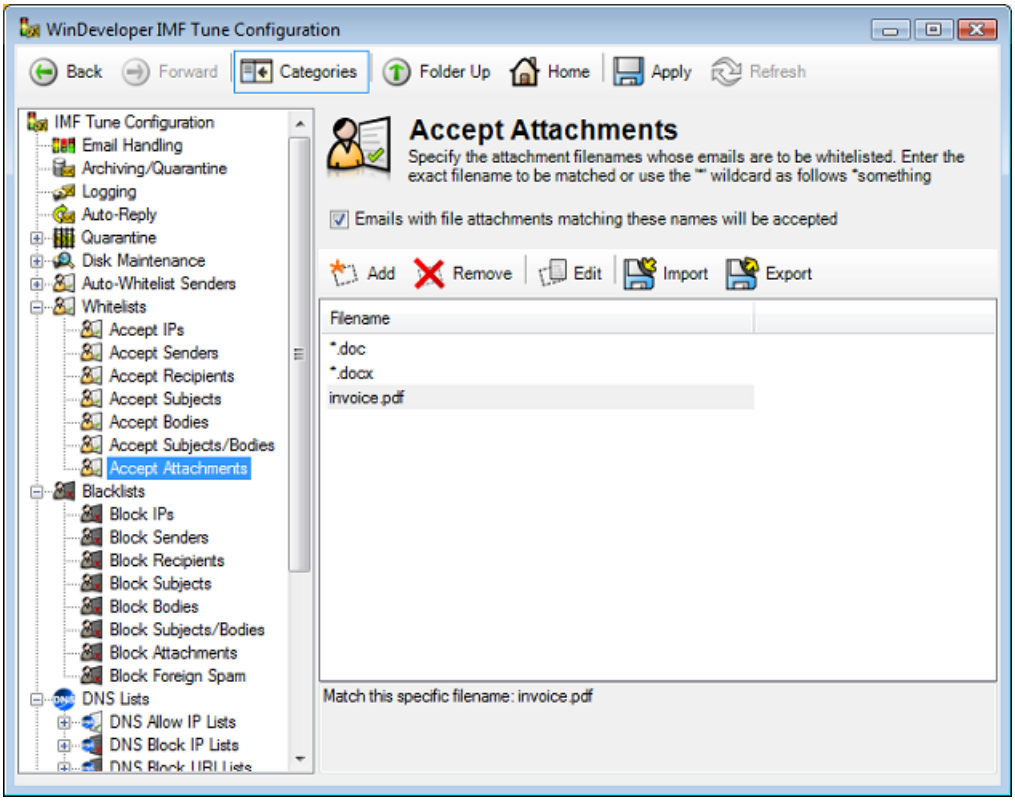
4.8.3.4 Exporting IPs

IMF Tune also supports exporting IP lists to an external text file. The export is correctly formatted to the IMF Tune import specifications. Thus we may use the export and import functionality in order to quickly replicate configurations on multiple IMF Tune installs.

Exports are always encoded in UTF-8. For details on the format of the exported file refer to Importing IPs.

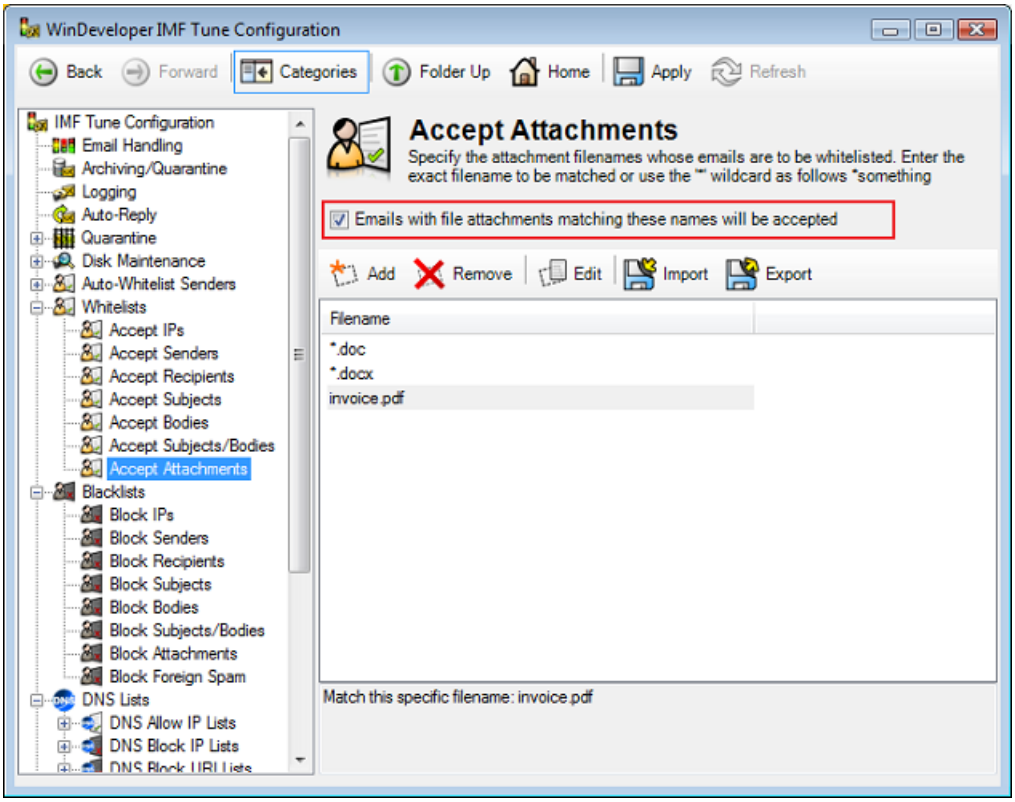
4.8.4 Accept Attachments

The Accept Attachments category enables the whitelisting of email attachments. IMF Tune attempts to match attachment names against this list. If a match is found the email is whitelisted.



4.8.4.1 Working with the Attachment List

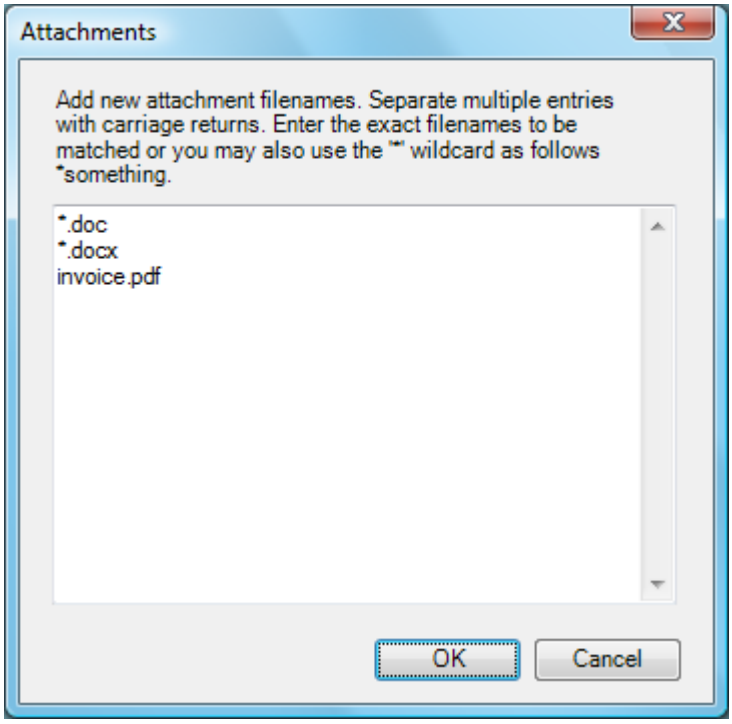
To enable/disable the attachment list set/clear the checkbox at the top. Setting the checkbox will activate the list and IMF Tune will process the attachment names against incoming emails.



Next we can add, remove and edit attachment names using the buttons at the top of the list.

4.8.4.2 Adding New Attachments

To add new attachment names click on the Add button. A dialog opens where multiple names may be entered:


Attachments
Add new attachment filenames. Separate multiple entries with carriage returns. Enter the exact filenames to be matched or you may also use the '*' wildcard as follows *something.
*.doc
*.docx
invoice.pdf
OK
Cancel

Enter each name in a separate line by hitting the carriage return key. The list can handle up to 64Kb of data at a time. To enter more names click OK to save and close the dialog. Next click Add again to re-open the dialog and enter more filenames. Otherwise we may use the import functionality to quickly add large lists of filenames.

We may include all filenames with a specific extension using the * wildcard. The wildcard is only supported at the very beginning of the filename: ***something**

4.8.4.3 Importing Filenames

IMF Tune enables the insertion of filenames into white/black lists through the import functionality. For the import to work the source file must meet the following requirements:

1. Importing only supports plain text files. The file may be encoded in 7-bit ASCII, UTF-8 or UTF-16. Although two UTF encoding formats are supported, all characters are expected to be within the standard Windows 1252 character set.

2. Multiple filename entries must be separated by a carriage return line feed (CRLF) sequence. For files generated on non-Windows platforms the line feed only separator (LF) is also supported.

In order to see a sample of a correctly formatted file use the Export functionality.

The import process includes a validation procedure that could reject some of the entries being imported. For example if a filename contains illegal use of the * wildcard that entry would be rejected.

When importing a large number of filenames it may be difficult to determine which of these failed to be imported. For this reason, whenever importing, the ImportReport.log file will be generated. This file is located in the main IMF Tune program directory and is overwritten on each import. The log file will show how each of the imported entries was handled and whether or not the entry was rejected due to validation reasons.

4.8.4.4 Exporting Filenames

IMF Tune also supports exporting filenames to an external text file. The export is correctly formatted to the IMF Tune import specifications. Thus we may use the export and import functionality in order to quickly replicate configurations on multiple IMF Tune installs.

Exports are always encoded in UTF-8. For details on the format of the exported file refer to Importing Filenames.

4.9 Working with Blacklists

Blacklists identify emails to be handled as spam. This is most useful when dealing with spam that still manages to reach the recipient inbox. Blacklisting is applied only in case the email is not Whitelisted or set to some fixed SCL value by an SCL Rule.

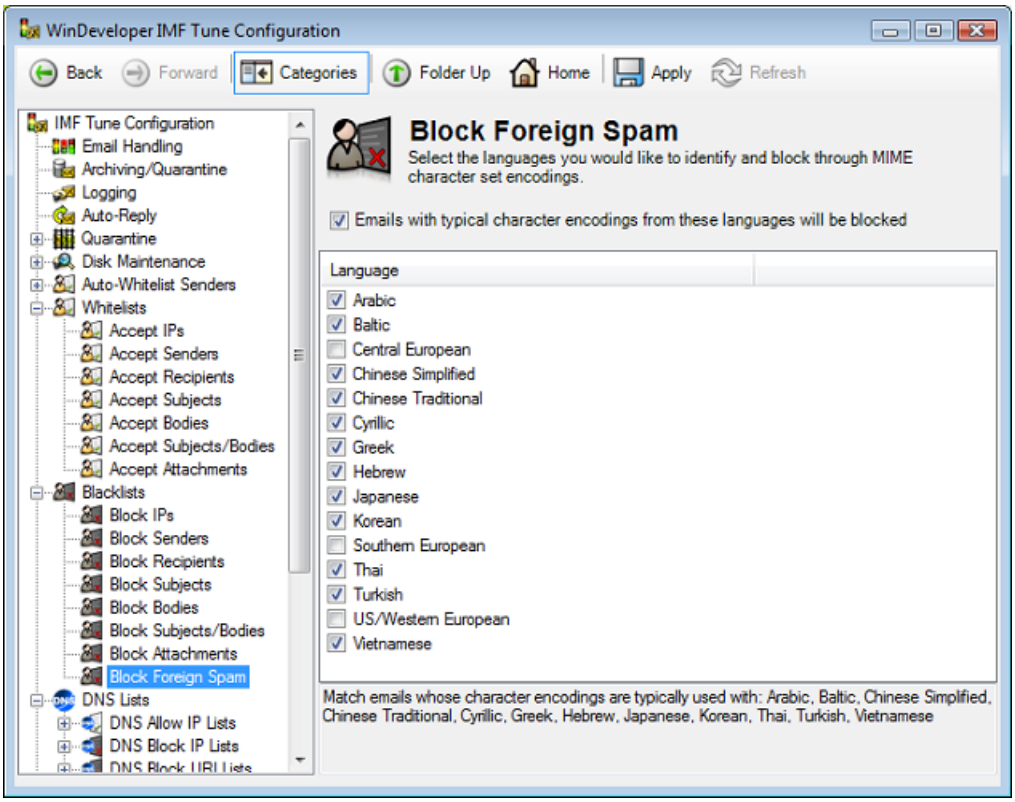
The Blacklists category groups IP, Sender, Recipient, Subject, Body, combined Subject/Body, Attachments and Language blacklisting.

IMF Tune provides a nearly identical set of whitelists and blacklists. The only difference is the Foreign Spam (Language) Blacklist. This has no corresponding whitelist.

Whenever a list type is present under both the Whitelist and Blacklist category group, the interface for the corresponding lists is identical. Hence for details on configuring the IP, Sender, Recipient, Subject, Body, combined Subject/Body and Attachment blacklists please refer to Working with Whitelists.

4.9.1 Foreign Spam Blacklist

The Foreign Spam blacklist filters emails by character set.



Emails can be authored in different languages with the help of character sets. A character set for a given language includes those characters and symbols in use for expressing that language.

In the Foreign Spam blacklist, IMF Tune provides a list of language categories. Selecting a language category, instructs IMF Tune to block emails authored using the character sets associated to it.

IMF Tune identifies the character sets by analyzing the encodings in use within the various email headers and the bodies.

Configuring this blacklist is just a matter of setting the checkboxes of the Language categories to block.

4.10 DNS List Filtering (Exchange 2007/2010/2013)

DNS List filtering is only supported in IMF Tune for Exchange 2007, 2010 and 2013. For Exchange 2003 we recommend using the Exchange Connection Filter.

DNS Lists open another window of information helping us to better identify spam and legitimate emails. List providers gather information using various listing criteria and publish their data for public consumption using the standard DNS infrastructure.

The most popular DNS List type is the one listing IPs of known spam sources. Other list types also exist. IMF Tune supports three of these:

- **DNS IP Whitelists** – IPs of known legitimate senders. Some of these may be engaged in opt-in email marketing.

- **DNS IP Blacklists** – IPs of hosts involved in the distribution of spam and other unsolicited emails.

- **DNS URI Blacklists** – URIs found in the body of spam emails. Typically these link back to spammers trying to sell a service or deliver other content over the internet.

Apart for listing different information, DNS Lists also differ from each other in other ways. Some of these differences include:

- **Price** – Some are free but others are available against payment

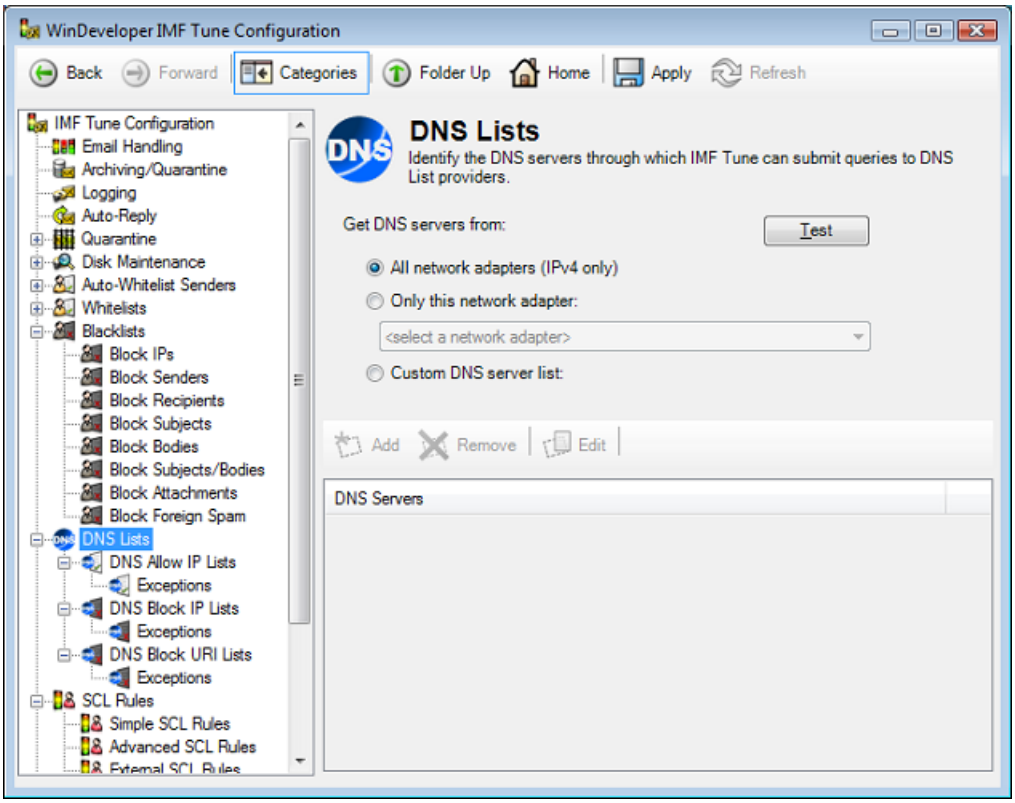
- **Accuracy** – Their effectiveness in identifying spam/legitimate emails varies (false positives/negatives)

- **Responsiveness and Availability** – The response time and uptime of the DNS list servers

It is important to be aware of these differences. Subscribing to a list that is not well maintained can adversely affect filtering.

4.10.1 DNS Server Configuration

IMF Tune requires some network information in order for it to submit DNS queries. Under the **DNS | Lists** category we identify the servers available for IMF Tune to connect to the DNS. IMF Tune uses these as a stepping stone to the DNS Lists.



Under *'Get DNS servers from'* we can choose:

- **All network adapters (IPv4 only)** – IMF Tune will automatically discover all network adapters and read the DNS settings from them.

- **Only this network adapter** – From the drop down list that follows, select a network adapter from which IMF Tune is to read the DNS configuration. When multiple network adapters are installed, one might be pointing at the internal DNS, whereas another might be pointing to the internet facing DNS. Since IMF Tune has to connect to external DNS Lists, we would select the internet facing network adapter.

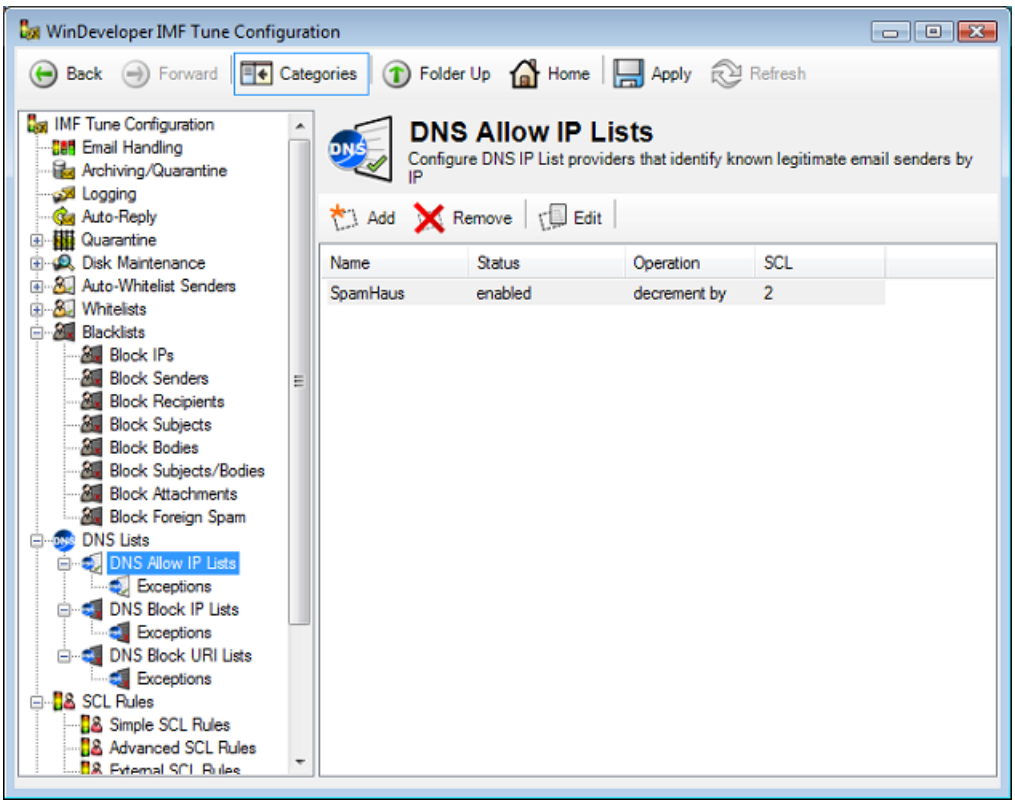
- **Custom DNS server list** – Specify one or more DNS server IPs at the list that follows. Use the Add, Remove and Edit buttons to update this list. Only IPv4 is allowed.

Note: If IMF Tune is configured to read network adapter settings, changes at the network adapter DNS configuration require an IMF Tune Engine service restart.

4.10.2 DNS IP Lists

IMF Tune supports both DNS IP Allow lists and Block lists. We discuss both of these here since the configuration elements are almost identical. To begin go to the configuration nodes:
DNS Lists | DNS Allow IP Lists
DNS Lists | DNS Block IP Lists

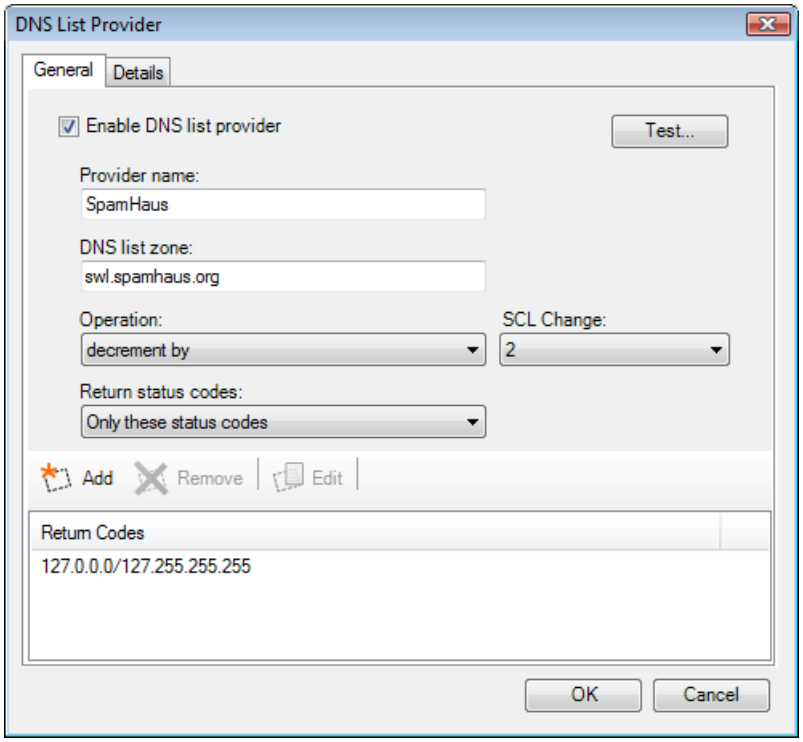
At the DNS IP List configuration we configure the details of the DNS List providers we want to query.



We manage List providers using the Add, Remove and Edit buttons.

4.10.2.1 Adding/Editing DNS IP List Providers

At the DNS Allow IP Lists/DNS Block IP Lists category click Add to open the DNS List Provider configuration dialog.



The List Provider configuration includes:
Provider name – A display name used to report matches in Keyword Reporting and at the IMF Tune Moderator.

DNS list zone – The DNS zone to be queried. This setting is supplied by the List Provider.

Operation/SCL Change – The change in SCL to be applied when the email source IP is found to be listed.

In DNS Block Lists choose an Operation from *'set value to'* or *'increment by'*. The former replaces the current SCL with the one configured under SCL Change. The latter applies an increment, raising the current SCL.

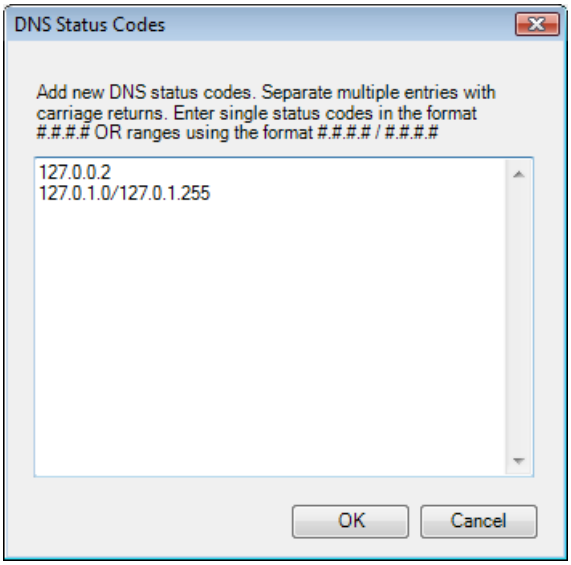
In DNS Accept Lists choose an Operation from *'set value to'* or *'decrement by'*. So we can either replace or lower the current SCL.

Return status codes – Identifies the possible response status codes the DNS List returns when a match is found. This information is supplied by the List Provider. By default any answer response code is interpreted as a match. However it is possible to configure a list that only matches specific response codes.

The Status Codes list is enabled whenever 'Return Status codes' is set to *'Only these status codes'*.

It is normal for DNS Lists to return status codes where the first octet has the decimal value of 127. For this reason in the above screenshot we configured IMF Tune to register a match whenever the status code starts with 127 (i.e. range: 127.0.0.0/127.255.255.255).

To add new status codes click the Add button to open the DNS Status Codes dialog.


DNS Status Codes
Add new DNS status codes. Separate multiple entries with carriage returns. Enter single status codes in the format #.#.#.# OR ranges using the format #.#.#.# / #.#.#.#
127.0.0.2
127.0.1.0/127.0.1.255
OK
Cancel

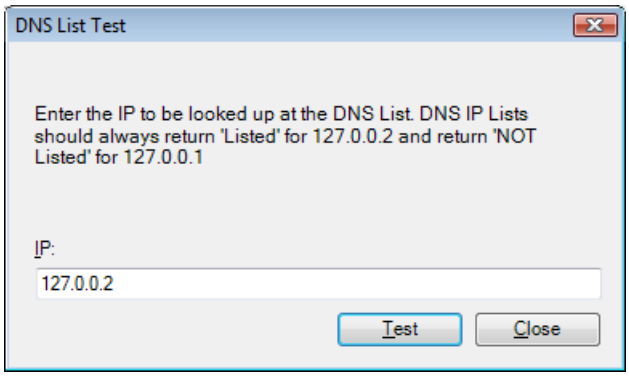
Here we can add single status code values in the IPv4 format or status code ranges in the format xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy (lower value limit/upper value limit). Ranges are inclusive of the limit values.

We can mix single status code values and ranges as needed. We just separate multiple entries with a carriage return.

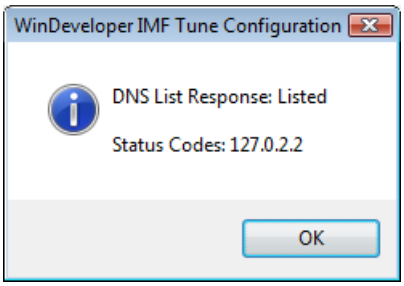
4.10.2.2 DNS IP List Provider Testing

From the DNS List Provider configuration dialog we can also submit test queries.

At the DNS Block IP Lists or DNS Allow IP Lists category click Edit to open one of the configured List Providers (or click Add and configure a new one). Next click the Test button to open the *DNS List Test* dialog.


DNS List Test
Enter the IP to be looked up at the DNS List. DNS IP Lists should always return 'Listed' for 127.0.0.2 and return 'NOT Listed' for 127.0.0.1
IP:
127.0.0.2
Test
Close

Enter the IP to be looked up and click Test.



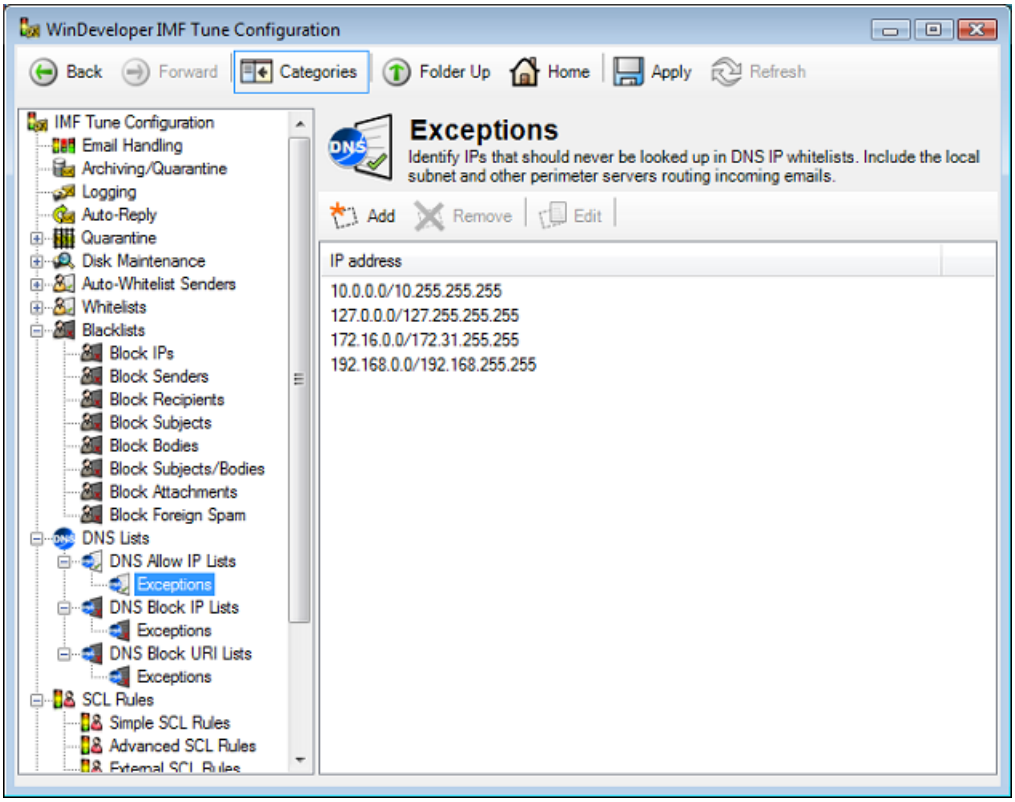
All DNS IP Lists support these standard test IPs:
127.0.0.2 – should always return Listed
127.0.0.1 – should always return NOT Listed

It is good practice to try these out whenever checking a DNS IP List. If the expected response is not returned, double check the setting under: DNS List Provider | DNS list zone

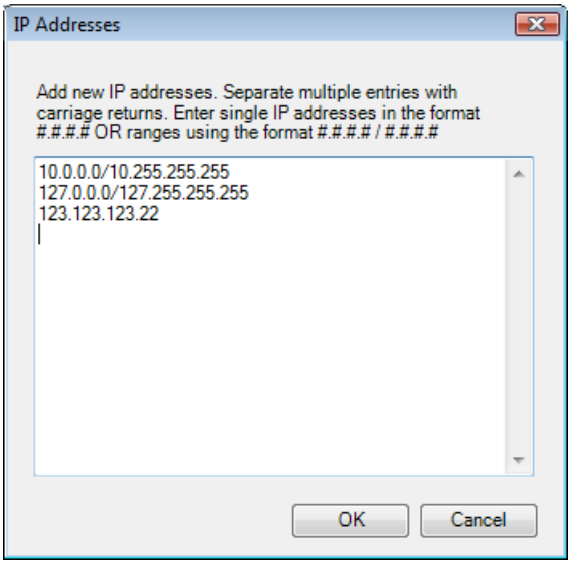
Apart for the standard test IPs, from here we can also test any other IP. We could verify our own public IP or check IPs shown at the IMF Tune logs for example.

4.10.2.3 DNS IP Exception List

Under the DNS Block IP Lists and DNS Allow IP Lists categories we have the Exceptions categories. Basically here we enter IPs that should skip DNS List filtering.



IMF Tune initializes the Exceptions list with standard IP ranges used in local subnets. To these we should add any other IPs used in routing incoming emails. We may also add other foreign IPs that should skip DNS List filtering here. To add new IPs to this list click the Add button.


IP Addresses
Add new IP addresses. Separate multiple entries with carriage returns. Enter single IP addresses in the format #.#.#.# OR ranges using the format #.#.#.# / #.#.#.#
10.0.0.0/10.255.255.255
127.0.0.0/127.255.255.255
123.123.123.22
OK
Cancel

Here we can enter single values in the IPv4 format or ranges in the format xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy (lower IP limit/upper IP limit). We can mix single IPs and ranges as needed. We just separate these with a carriage return.

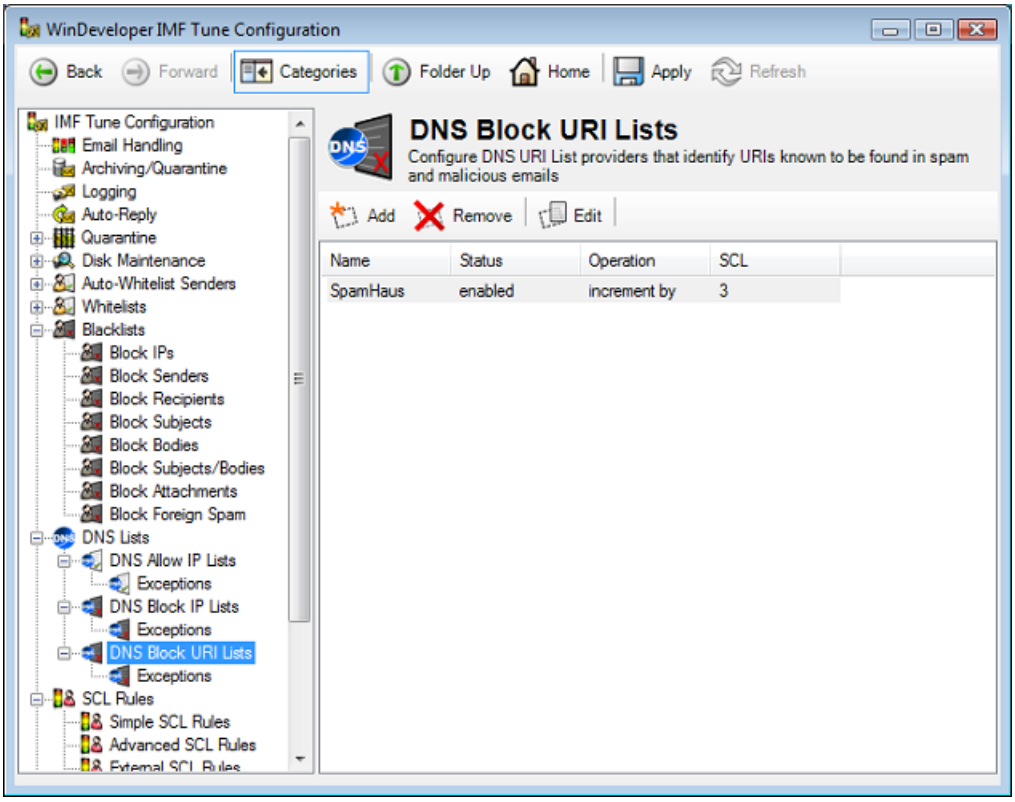
4.10.3 DNS URI Lists

DNS URI Lists allow us to test if links within the email body point to sites affiliated to spammers.

Spammers wanting to sell something provide links to their order pages. A phishing email normally links to a site where users are tricked to hand over their personal data. Other spam emails use links to download images from the internet. In all cases links are a very important hook for a spammer to reach his goal.

IMF Tune will dig links from the message body and submit them to the DNS URI Block list of our choice. To begin go to:
DNS Lists | DNS Block URI Lists

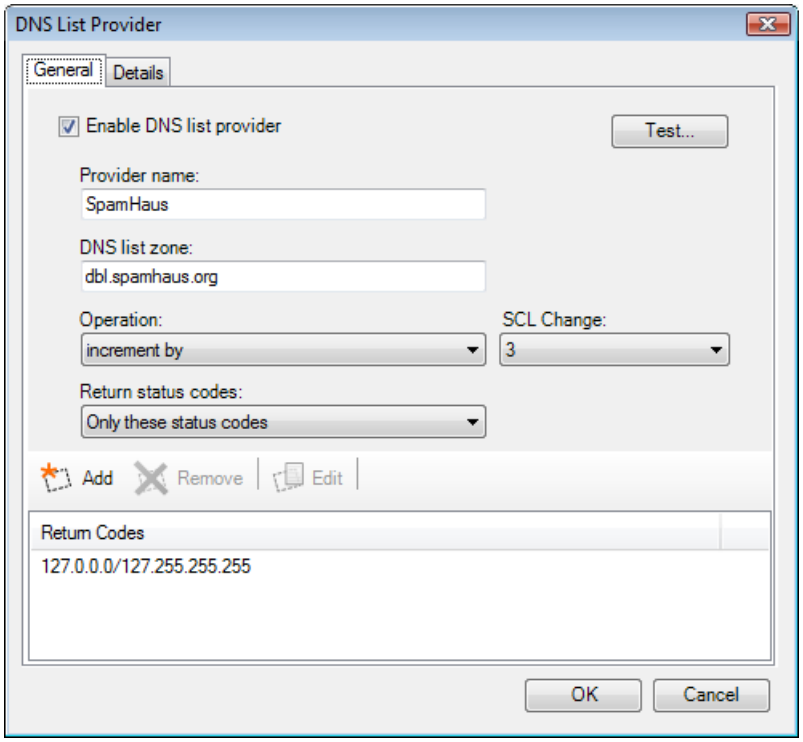
Here we configure the details of the DNS URI List providers we want to query.



We manage List providers using the Add, Remove and Edit buttons.

4.10.3.1 Adding/Editing DNS URI List Providers

At the DNS Block URI Lists category click Add to open the DNS List Provider configuration dialog.

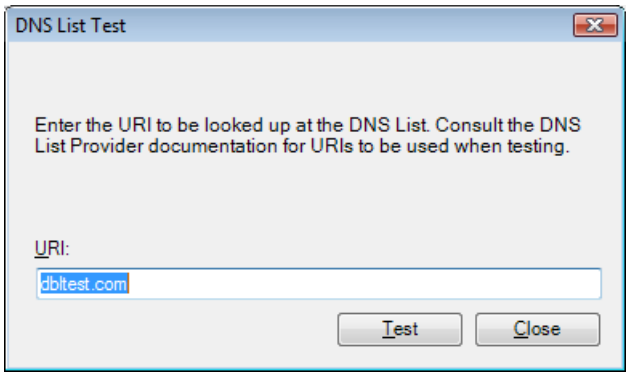


The options here are identical to those for DNS Block IP Lists. For more details on how to configure the list provider check *Adding/Editing DNS IP List Providers.*

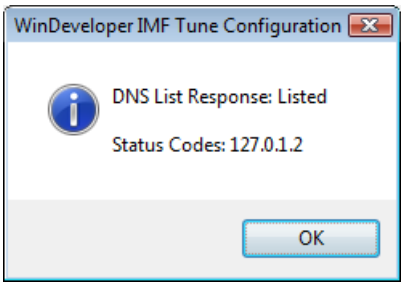
4.10.3.2 DNS URI List Provider Testing

From the DNS List Provider configuration dialog we can also submit test queries.

At the DNS Block URI Lists category click Edit to open one of the configured List Providers (or click Add and configure a new one). Next click the Test button to open the DNS List Test dialog.


DNS List Test
Enter the URI to be looked up at the DNS List. Consult the DNS List Provider documentation for URIs to be used when testing.
URI:
dbltest.com
Test
Close

Enter the URI to be looked up and click Test.



Unlike DNS IP Lists, URI Lists do not consistently adopt the same test URI to be used when testing the list. Each provider defines his own test URI. IMF Tune automatically initializes the Test dialog with the correct test URI for most providers. However it is always recommended to check the provider documentation.

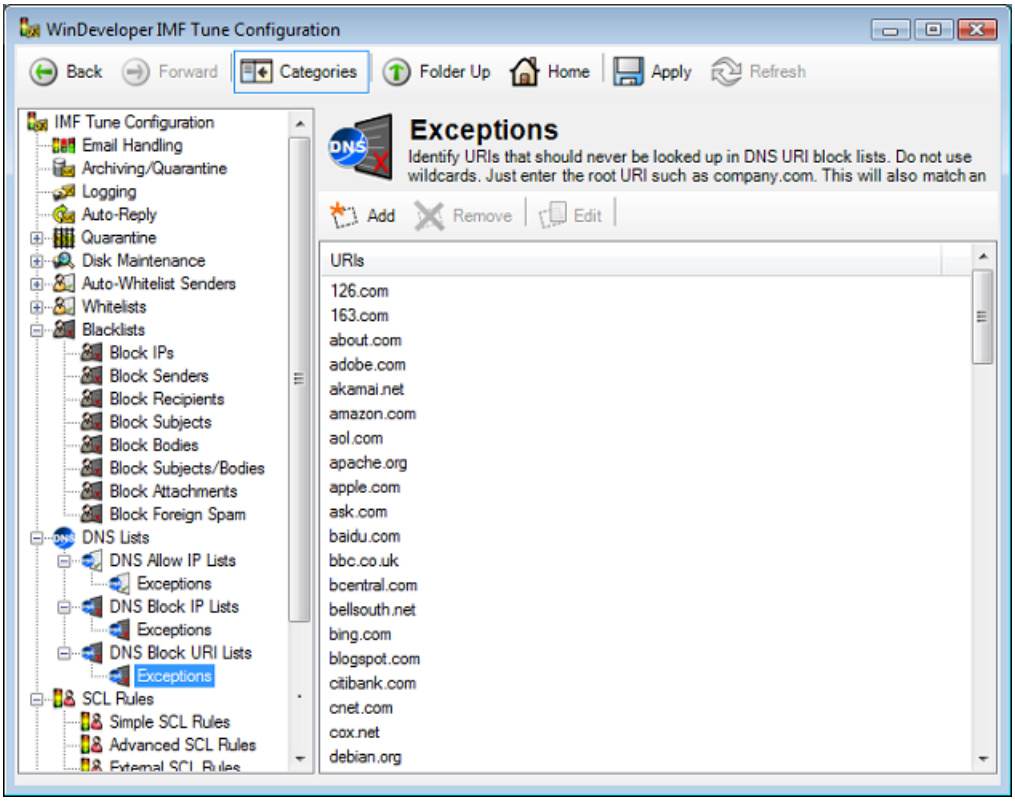
Apart for testing the designated test URI, we can of course also test any other URI. If the expected response is not returned, double check the setting under: DNS List Provider | DNS list zone

When testing URIs it is recommended to just use the root part of the URI. For example if I have the link http://www.windeveloper.com/imftune, at the test dialog I would just enter windeveloper.com

Some URI List providers require the use of the root portion others don't have this requirement.

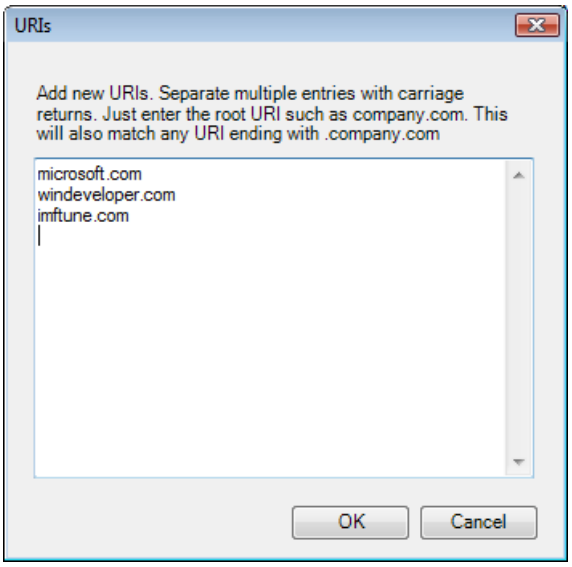
4.10.3.3 DNS URI Exception List

Under the DNS Block URI Lists category we have the Exceptions category. Basically here we enter URIs that should skip DNS List filtering.



The Exception list is initialized with URIs of well-known domains that may safely skip processing. Exceptions eliminate many DNS queries and thus are beneficial in improving scanning performance. We recommend adding entries to this list starting from your own public domains referred by users in their everyday work.

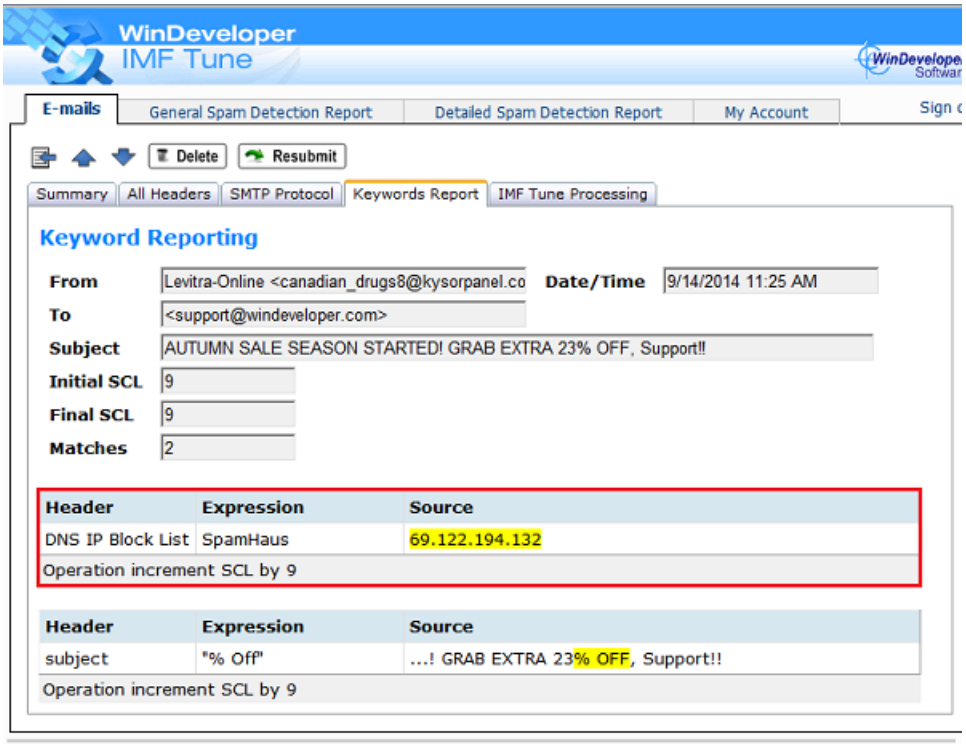
To add new URIs to the Exception list click the Add button.


URIs
Add new URIs. Separate multiple entries with carriage returns. Just enter the root URI such as company.com. This will also match any URI ending with .company.com
microsoft.com
windeveloper.com
imftune.com
OK
Cancel

Here enter the root URI such as windeveloper.com. This will also match any URI with the same root such as *www.windeveloper.com* or *some.other.windeveloper.com*

4.10.4 DNS List Reporting

Keyword Reporting and the Moderator/Reporting Web Interface will also report on DNS List matches. This is how a DNS Block IP List match looks like at the Moderator:



At the report we can see:
Header – shows the type of DNS List involved in this case a DNS IP Block List.

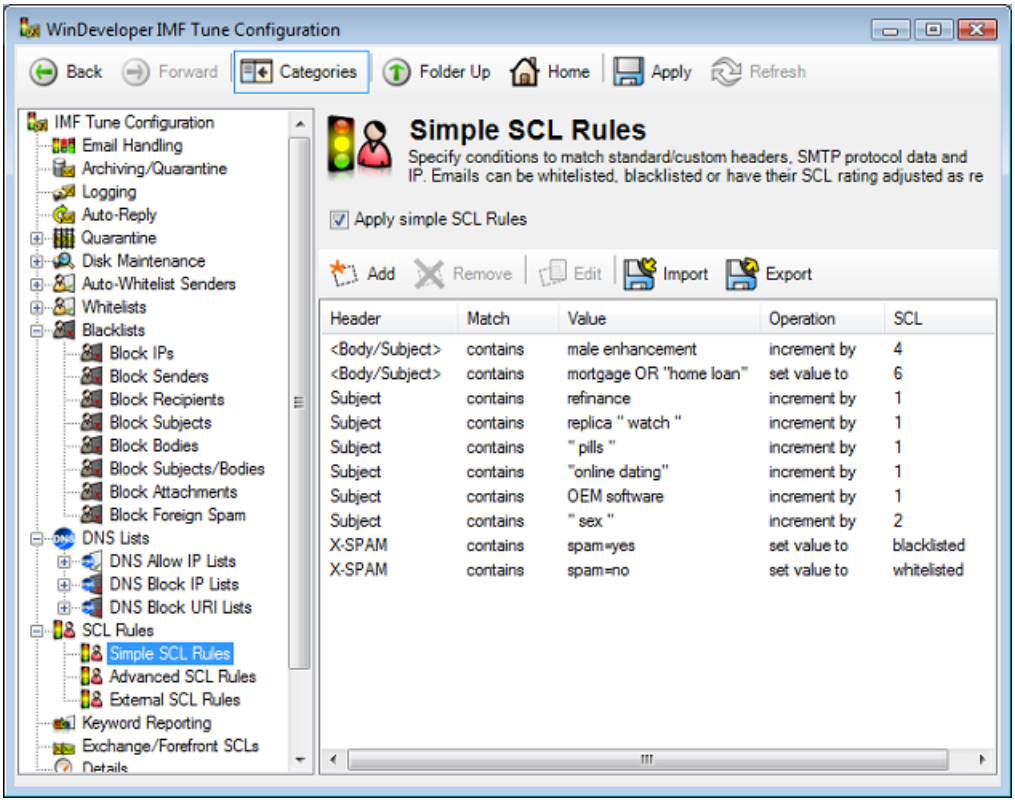
Expression – shows the Provider Name set at the DNS List Provider configuration.

Source – shows the actual email information that was matched. In this case we have the email originating IP.

Just like any other blocked email, emails blocked by DNS Block Lists can be resubmitted for delivery from the Moderator interface.

4.11 Simple SCL Rules

Simple SCL Rules allow the setup of keyword-to-SCL mappings. Conditions are tested against the sending host IP, addresses, attachment names, headers, bodies and the combined subject/body data.



On finding a match, the current SCL may be changed in one of the following manners:

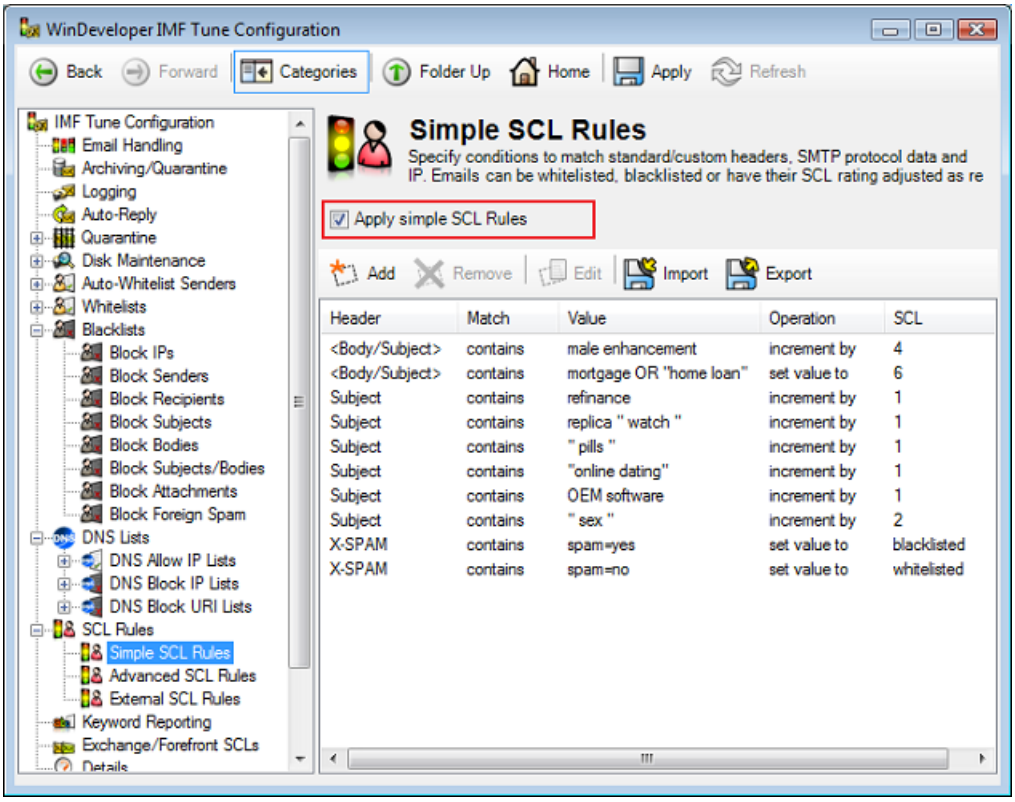
- Whitelisted, Blacklisted or replaced by any of SCL 0 to 9
- Incremented by a value from 1 to 9
- Decremented by a value from 1 to 9

SCL increments/decrements add up such that if multiple matches are found the final SCL is set to the net result.

Simple SCL Rules provide a more advanced alternative to the basic white/black lists. All of the email information processed by these lists is also processed by SCL Rules. In addition here we have more control on the assigned SCL. Furthermore we also have the opportunity to test against headers not covered by the white/black lists. For example one might search the Received headers for IPs.

4.11.1 Working with Simple SCL Rules

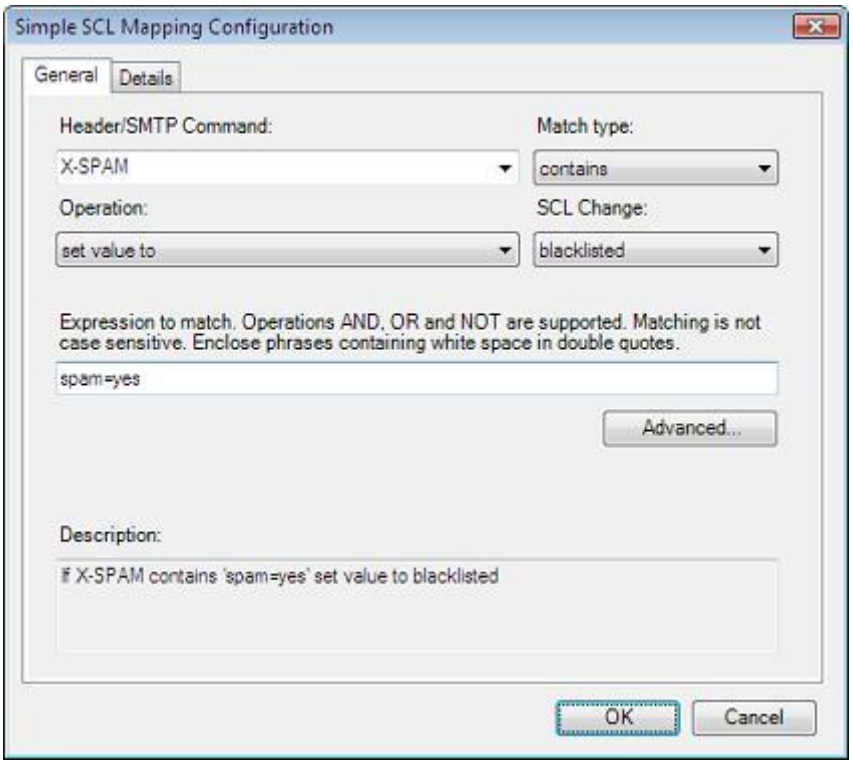
To enable/disable Simple SCL Rules set/clear the checkbox at the top. Setting the checkbox will activate the list and IMF Tune will process the configured rules against incoming emails.



Next we can add, remove and edit rules using the buttons at the top of the list.

4.11.2 Adding/Editing New SCL Mappings

To add new SCL Mappings click on the Add button. This will open the Simple SCL Mapping Configuration interface.



From here we can choose the email information to be analyzed, specify a condition to be matched, and select the operation to perform on matched emails. For a detailed discussion on using this interface check the SCL Mapping Configuration section.

4.11.3 SCL Mapping Configuration

The SCL Mapping interface provides two property pages. At the General page the various mapping options are available. At the Details page, the configuration keeps track of the creation and last modification date for the mapping. It also provides space for an administrative note.

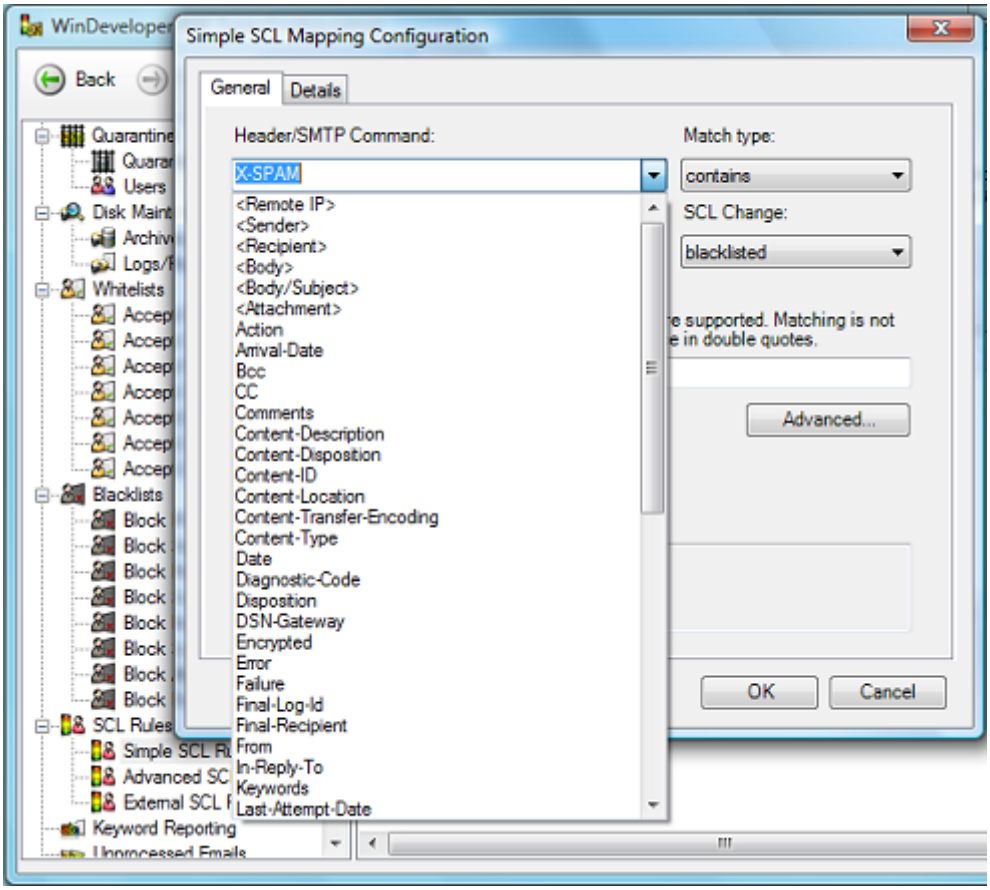
A mapping is composed of three pieces of information:

- the type of email information to analyze
- keywords/data to be matched against processed emails
- the operation to perform on finding a match

We discuss how to configure these three components in the sections that follow.

4.11.3.1 Identifying the Email Information Type

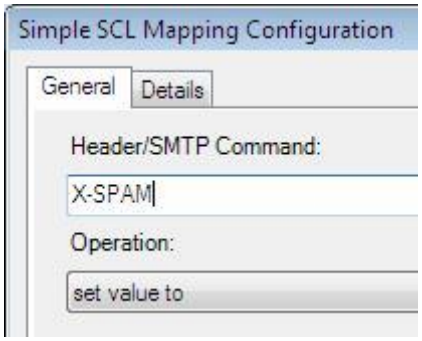
Each SCL Mapping must be processed against some specific piece of information within the analyzed emails. The 'Header/SMTP Command' combo box lists various email information types.



The above screenshot shows some of the options available at this list. Here entries not identifying email headers are enclosed in triangular brackets. The list includes:

- Remote IP
- Sender and Recipient Addresses
- Email bodies
- Combined Subject/Body data
- Attachment names
- Various standard email headers

Mappings against non-standard (custom) email headers may also be configured. In this case just type the header name directly into the combo box:

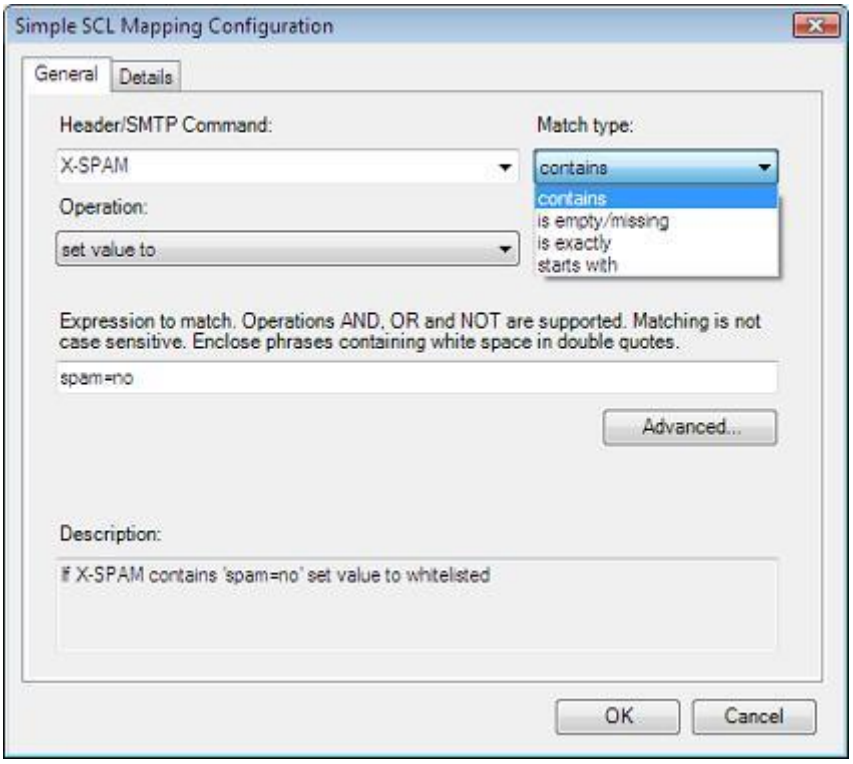


Note that for a single email, the sender address may be identified in a number of ways. IMF Tune checks all of these locations:

- MAIL FROM protocol address
- From header
- Sender header
- Resent-From header
- Resent-Sender header

4.11.3.2 Choosing a Match Type

The Match Type dropdown list box is available when setting up mappings against standard or custom email headers.



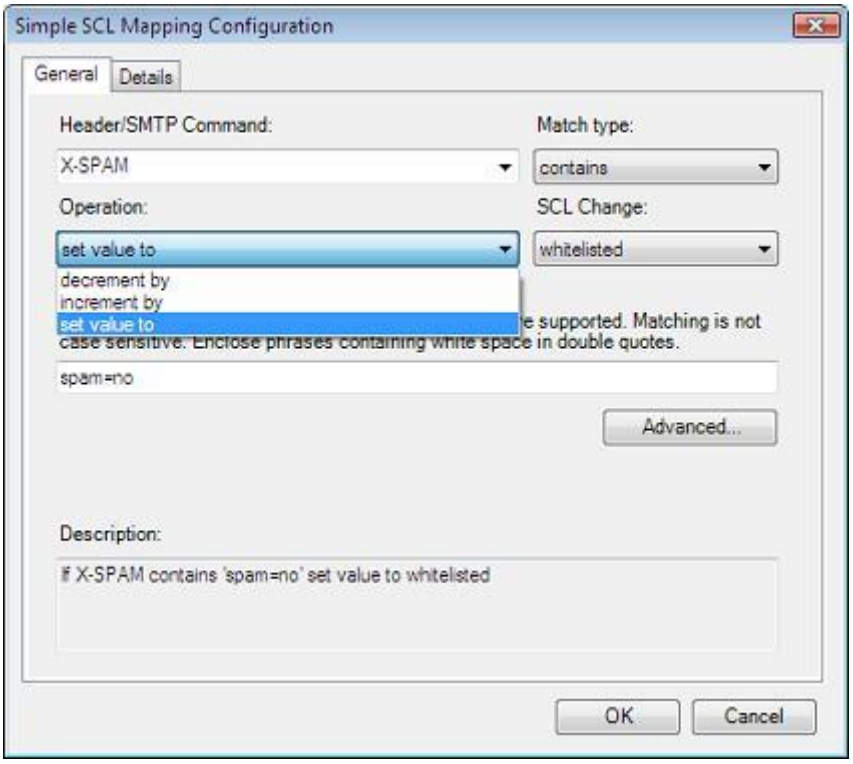
The list identifies the type of matching operation to be performed when analyzing emails against this rule. The following matching operations are possible:

contains	The header must match the keyword expression specified in the value edit box. The expression may include the use of the AND, OR, NOT operators, and double quotes. For details on keyword expression check Constructing Search Expressions.
is empty/missing	The mapping is matched if the header is not found, or is empty valued.
is exactly	The header must have exactly the same value specified in the value edit box ignoring any extra white-space. Operators are not supported and any value entered will be matched literally.
starts with	The header value must start with the text specified in the value edit box ignoring any extra white-space. Operators are not supported and any value entered will be matched literally.

4.11.3.3 Performing an SCL Change Operation

Once IMF Tune establishes that a specific mapping matches an email, the current SCL value will be modified based on the type of Operation configured. Here an operation is composed of an Operation type and an SCL value.

The Operation dropdown list box provides a selection of operation types:

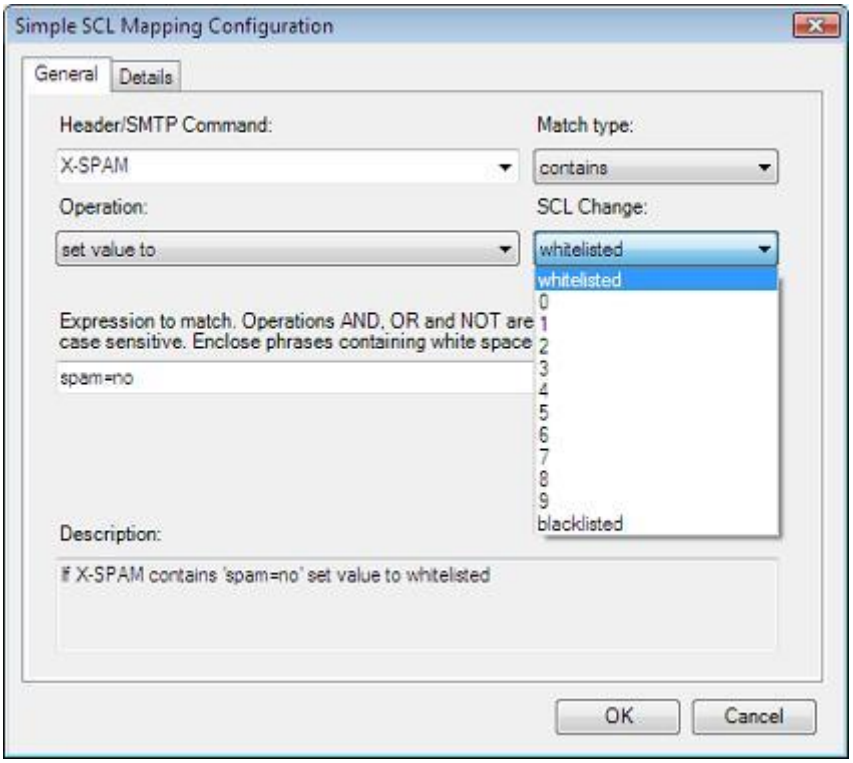


The following summarizes the meaning for each of these operation types:

decrement by	Decrement the current SCL value by the specified amount.
increment by	Increment the current SCL value by the specified amount.
set value to	Replace the current SCL value by another value.

Each operation requires an SCL increment, decrement or a new SCL value to be applied. Valid increments/decrements range from 1 to 9. Valid overriding SCL values include whitelisted, blacklisted and SCL 0 to 9.

Choose this value from the SCL change dropdown list box:



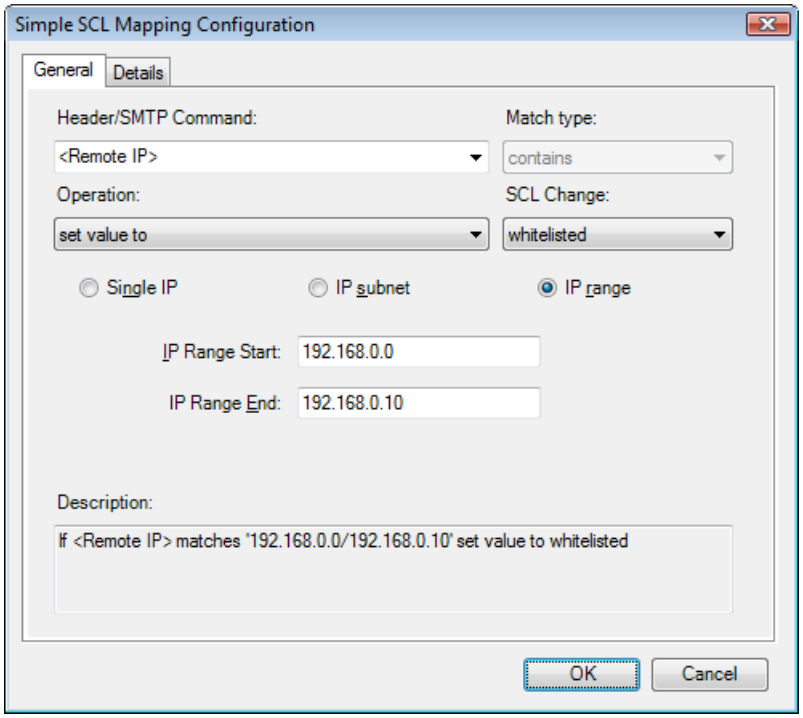
Applying SCL increments/decrements enables us to directly influence the way emails are rated. If we feel that some form of spam is not being rated high enough, then we can identify keywords and allocate an SCL increment to it.

Using ‘set value to’ we may white/black list emails or choose to set the SCL to any other absolute value. In this manner emails can be forced to go to the Junk Email folder for example. Indeed based on how the SCL thresholds were configured under the Email Handling category, the exact type of operation to be applied can be selected by forcing a specific SCL value.

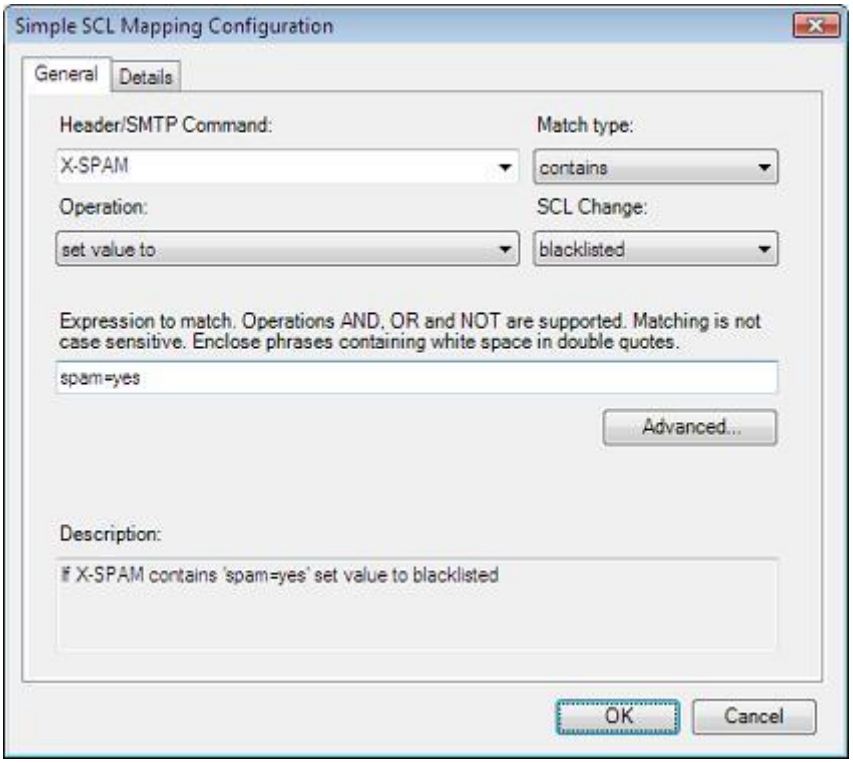
4.11.3.4 Specifying Expressions/Data to Match

Unless we are trying to map an empty/missing header, the SCL Mapping dialog will provide the necessary interface to enter the data to be matched.

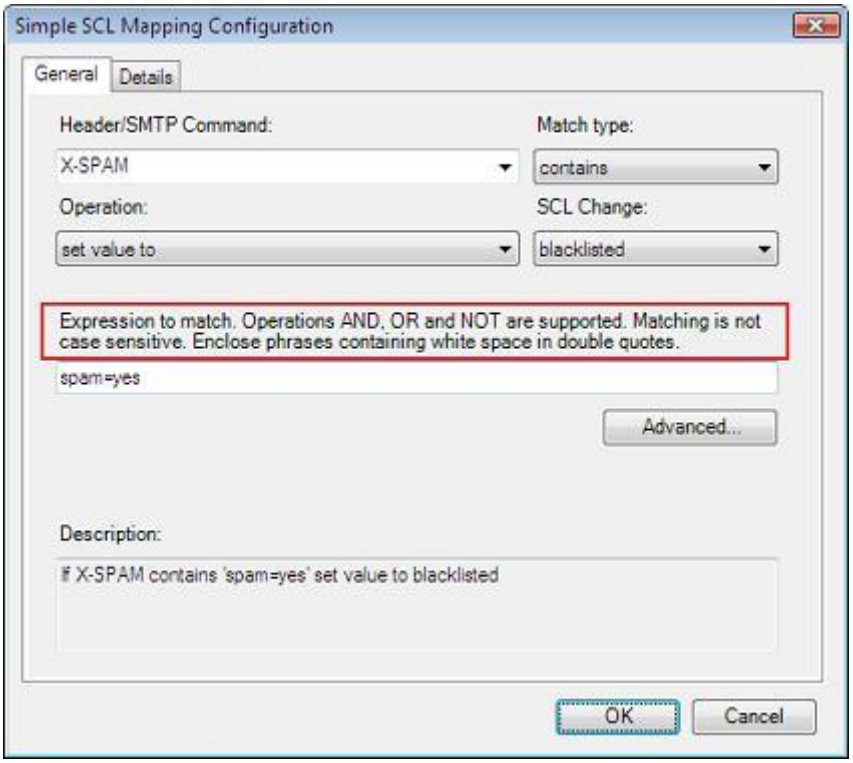
This interface will change depending on the type of email information being mapped. For example, on mapping the sending host IP the interface provides for entering a single IP, an IP range or an IP/Mask pair.



On the other hand on mapping against email headers a keyword expression is required. In this case a simple edit box is presented for entering the necessary text. Here the Advanced button is also enabled. This brings up the Expression Builder interface enabling easy construction of complex expressions.



To facilitate data entry the interface will also dynamically update the information summarizing what type of data is expected. This is handy because of the change in requirements taking effect as we configure the other SCL Mapping options:



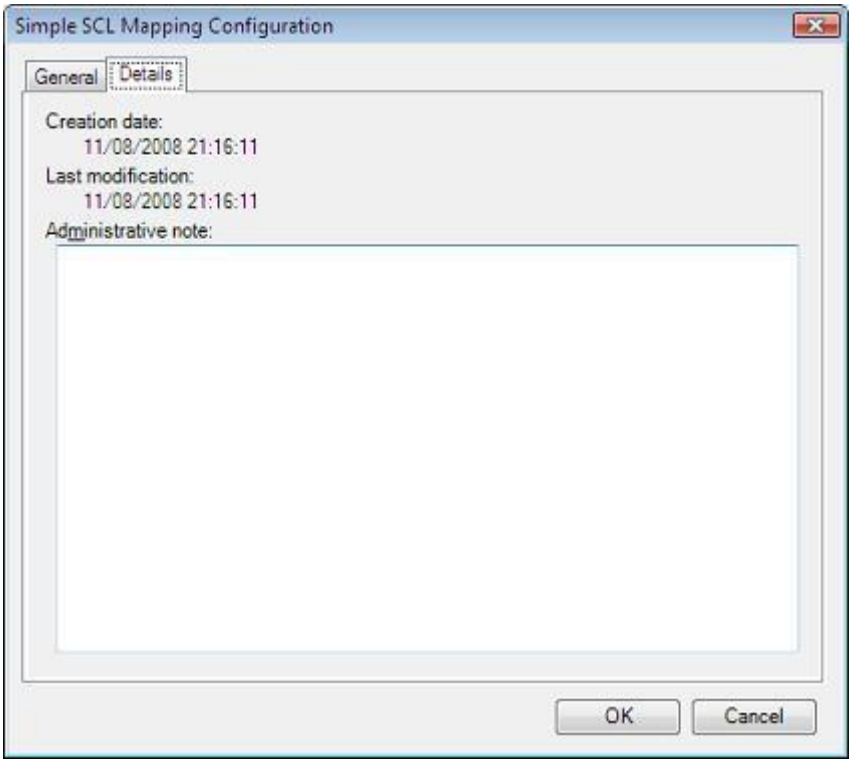
The following table summarizes the type of information expected for various types of mappings:

<Remote IP>	Choose between a single IP, an IP range or an IP/Mask pair.
<SMTP Sender> <SMTP Recipient>	Enter an email address in the format something@something. We may also use wildcards to match addresses by domain: *@domain *@*.domain
<Body> <Body/Subject>	Enter a keyword expression. Operators AND, OR, NOT and double quotes are supported. Click on the Advanced button to use the Expression Builder. Check the sections Constructing Search Expressions and Working with the Expression Builder for more details.
<Attachment>	Enter the exact filename or use the * wildcard as follows: *something
Standard or Custom Headers	When mapping against email headers the matching type adds some more options. All possible combinations follow: **contains** – Enter a keyword expression. Same as for <body> **is empty/missing** – No value is required. **is exactly, starts with** – Enter the exact text to be matched. All text will be matched literally and operators are not supported.

4.11.3.5 Details

For each of the configured SCL mappings, IMF Tune will keep track of the creation and last modification dates. Furthermore the configuration provides the space for administrative notes to be inserted. In this manner changes may be documented for future reference.

To specify a comment under the SCL Mapping configuration, select the Details page and enter the text under the Administrative note edit box:



4.12 Advanced SCL Rules

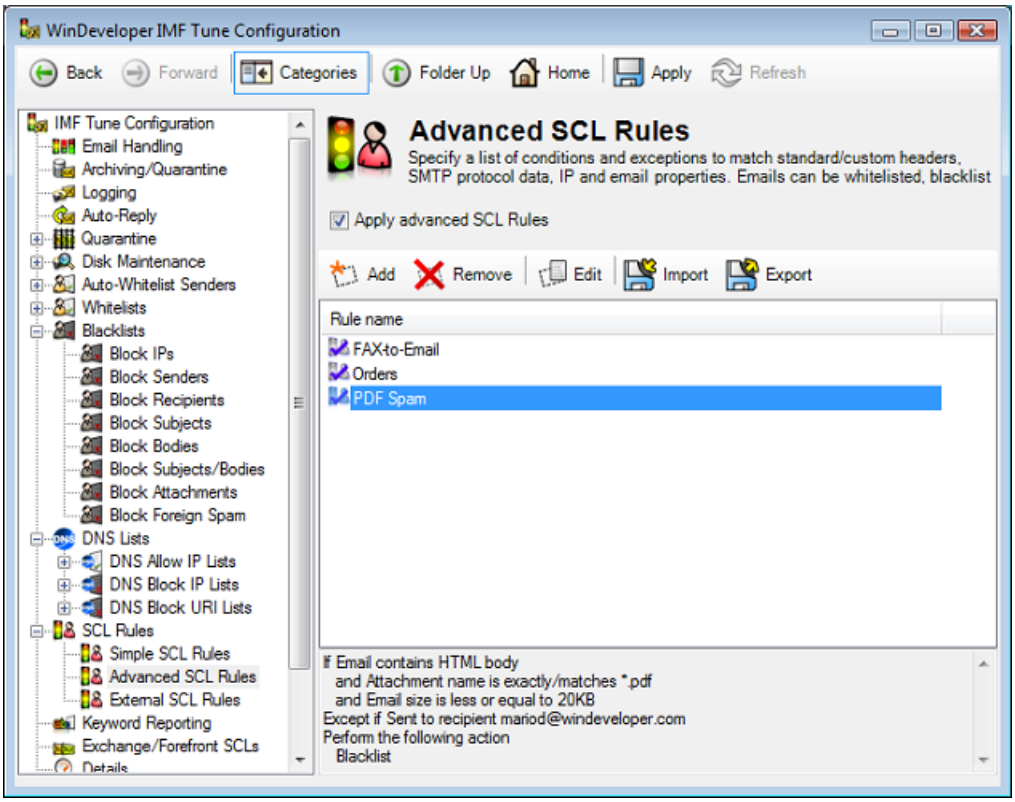
Advanced SCL rules bring even more power. Rules here are composed of multiple conditions and exceptions that must be satisfied for the action to be applied. In this manner, for example, we could create a subject whitelist that is only applied to a number of recipients. Indeed the ability to combine multiple conditions together adds a new level of flexibility.

Advanced SCL Rules also give access to other email properties not available from anywhere else within IMF Tune. Some examples include the email size, the recipient count, the reception time and others.

Just like Simple Rules, the action set allows for incrementing/decrementing the SCL rating and for setting it to any fixed value including the whitelist and blacklist levels. Thus the rules can be employed both as an advanced white/black list and to fine tune SCL assignments.

4.12.1 Working with Advanced SCL Rules

To enable/disable Advanced SCL Rules set/clear the checkbox at the top. Setting the checkbox will activate the list and IMF Tune will process the configured rules against incoming emails.



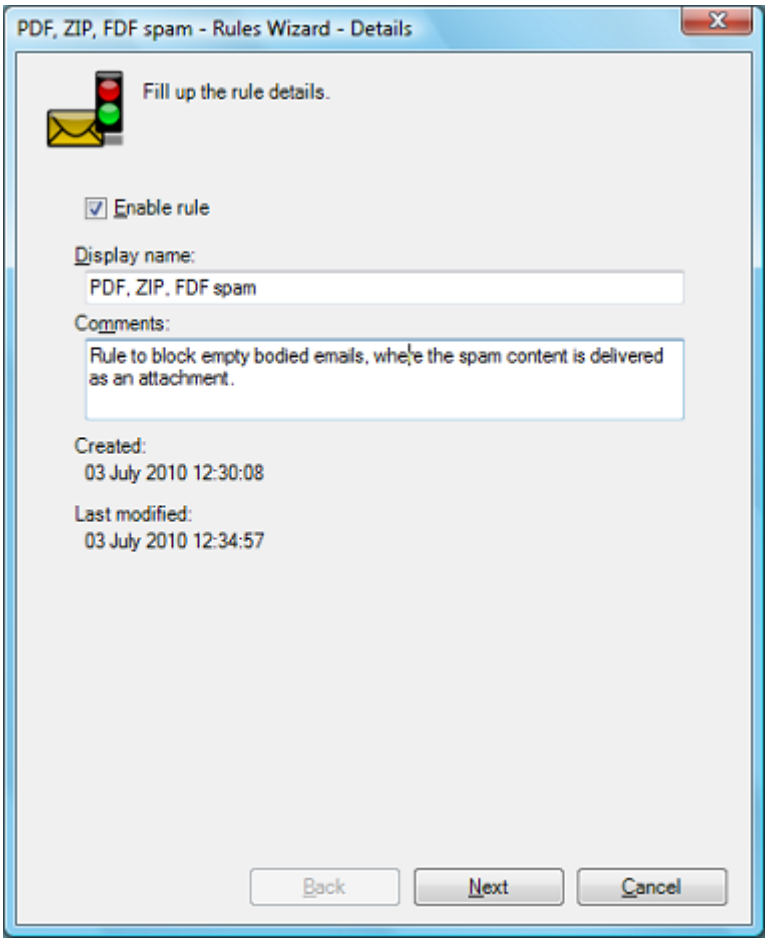
Apart for enabling/disabling the entire set of advanced rules, we can enable/disable individual rules. This can be done by opening the rule and setting/clearing the enablement checkbox shown later. Disabling a rule is handy especially if we only want to stop enforcing it temporarily.

Next we can manage the rule list using the Add, Remove and Edit buttons.

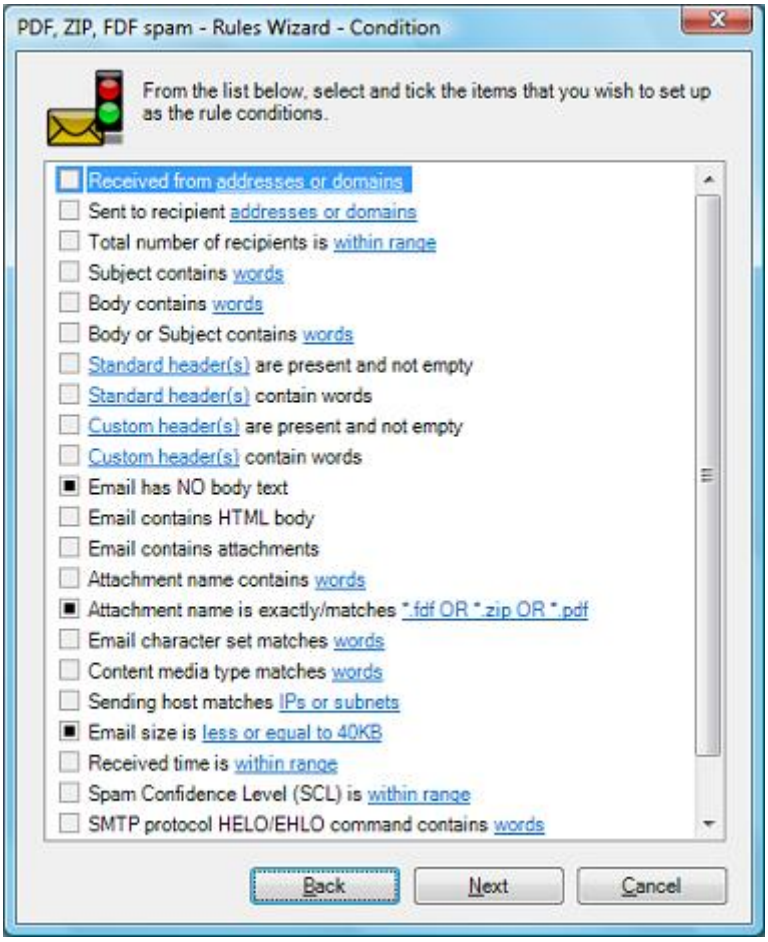
4.12.2 Adding Advanced SCL Rules

Click on the Add button to start creating a new Advanced rule. This will start the Advanced Rules Wizard. It provides the necessary steps for constructing rules composed of conditions, exceptions and an action. In order for the rule action to be applied the email must match all conditions, without matching any of the exceptions.

The Wizard starts from the Details page exposing some general properties. At the Display Name field a rule name must be supplied. Under Comments an administrative note may be entered, typically to describe the intent of the rule. The Enable rule checkbox controls the rule state. If cleared, the rule will be saved without being applied to any emails. At the bottom this page also shows the creation and last modified dates.



Clicking Next we move to the Conditions configuration page. Here we find various condition types that may be activated by setting the adjacent checkbox. An email must satisfy all of the selected conditions in order for the rule to be matched.

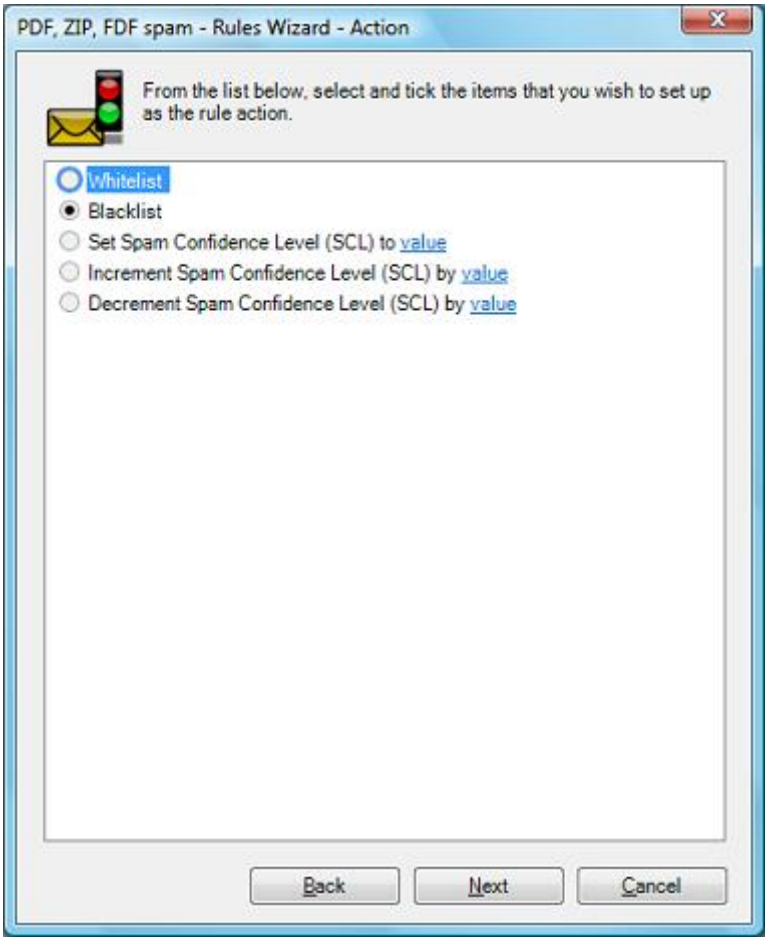

PDF, ZIP, FDF spam - Rules Wizard - Condition
From the list below, select and tick the items that you wish to set up as the rule conditions.
Received from addresses or domains
Sent to recipient addresses or domains
Total number of recipients is within range
Subject contains words
Body contains words
Body or Subject contains words
Standard header(s) are present and not empty
Standard header(s) contain words
Custom header(s) are present and not empty
Custom header(s) contain words
Email has NO body text
Email contains HTML body
Email contains attachments
Attachment name contains words
Attachment name is exactly/matches *.fdf OR *.zip OR *.pdf
Email character set matches words
Content media type matches words
Sending host matches IPs or subnets
Email size is less or equal to 40KB
Received time is within range
Spam Confidence Level (SCL) is within range
SMTP protocol HELO/EHLO command contains words
Back
Next
Cancel

Most conditions necessitate the configuration of additional properties. These include a link within the condition description that when clicked provide access to these properties.

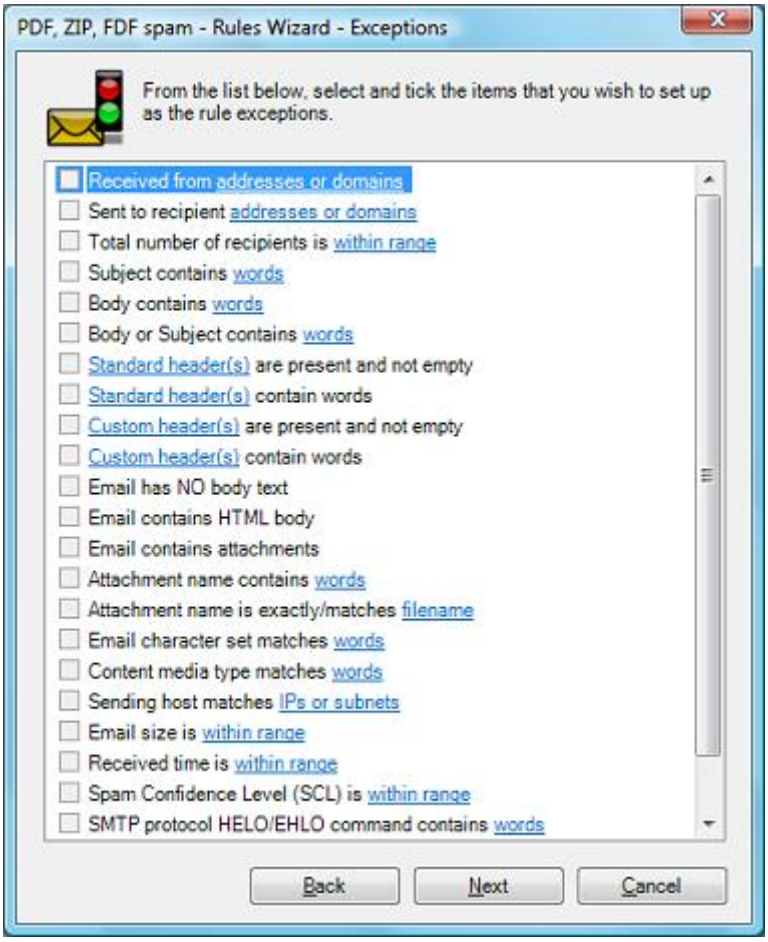
Clicking Next we move to the Action configuration page. Here we select the type of operation to be performed on matching the rule.

Just like in Simple Rules, the action is employed to adjust the current SCL rating in one of the following manners:

- Whitelist, Blacklist or replace by any of SCL 0 to 9
- Increment by a value from 1 to 9
- Decrement by a value from 1 to 9


PDF, ZIP, FDF spam - Rules Wizard - Action
From the list below, select and tick the items that you wish to set up as the rule action.
Whitelist
Blacklist
Set Spam Confidence Level (SCL) to value
Increment Spam Confidence Level (SCL) by value
Decrement Spam Confidence Level (SCL) by value
Back
Next
Cancel

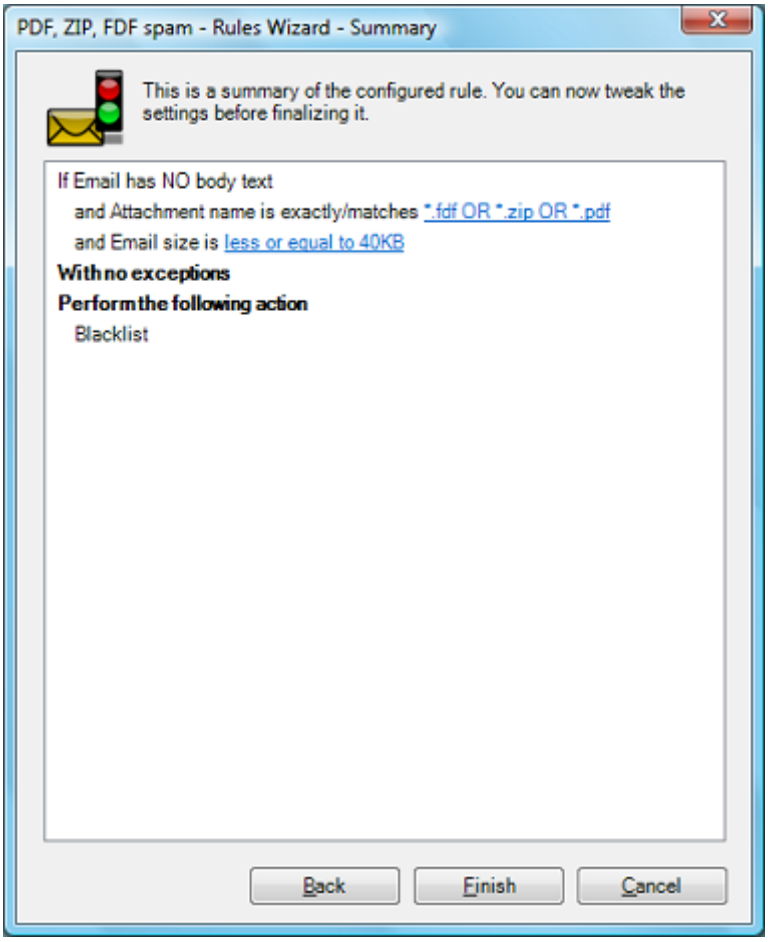
The Next Wizard page leads us to the Exception configuration step.


PDF, ZIP, FDF spam - Rules Wizard - Exceptions
From the list below, select and tick the items that you wish to set up as the rule exceptions.
Received from addresses or domains
Sent to recipient addresses or domains
Total number of recipients is within range
Subject contains words
Body contains words
Body or Subject contains words
Standard header(s) are present and not empty
Standard header(s) contain words
Custom header(s) are present and not empty
Custom header(s) contain words
Email has NO body text
Email contains HTML body
Email contains attachments
Attachment name contains words
Attachment name is exactly/matches filename
Email character set matches words
Content media type matches words
Sending host matches IPs or subnets
Email size is within range
Received time is within range
Spam Confidence Level (SCL) is within range
SMTP protocol HELO/EHLO command contains words
Back
Next
Cancel

The exceptions interface is identical to that for conditions. However exceptions have the opposite meaning i.e. for the rule action to be applied an email must not match any exceptions.

.

Clicking Next we reach the final Summary page. From here we can review all the conditions, exceptions and action type configured. This page also gives us the opportunity to revise and modify the rule settings. Editable properties are again accessible through links.


PDF, ZIP, FDF spam - Rules Wizard - Summary
This is a summary of the configured rule. You can now tweak the settings before finalizing it.
If Email has NO body text
and Attachment name is exactly/matches *.fdf OR *.zip OR *.pdf
and Email size is less or equal to 40KB
With no exceptions
Perform the following action
Blacklist
Back
Finish
Cancel

4.12.2.1 Condition/Exception Types

The conditions and exceptions lists provide access to various email properties. These include all properties available from white/black lists and Simple SCL Rules. Additionally Advanced Rules exposes some more properties that are unique to this interface.

The following is the list of condition/exception types available:

Condition/Exception Type	Description
Received from addresses or domains	Matches the email sender address. For a single email, the sender address may be identified in a number of ways. IMF Tune checks all of these locations: • MAIL FROM protocol address • From header • Sender header • Resent-From header • Resent-Sender header This condition supports using the * wildcard in order to identify an entire domain. In all one of these formats must be used: alias@domain *@domain *@*.domain
Sent to recipient addresses or domains	Matches email recipient addresses. This condition supports using the * wildcard in order to identify an entire domain. In all one of these formats must be used: alias@domain *@domain *@*.domain
Total number of recipients is within range	Matches the number of recipients the email is addressed to including any BCCs.
Subject contains words	Matches email subjects. This condition supports keyword expressions.
Body contains words	Matches text extracted from plain text and HTML bodies. Also processed against the raw HTML for matching of tags and other content that is normally invisible. This condition supports keyword expressions.

Body or Subject contains words	Matches text within the body or email subject. Used when the exact text location is not important. This condition supports keyword expressions.
Standard header(s) are present and not empty	Tests for the presence of standard headers.
Standard header(s) contain words	Matches text within any of the standard headers. This condition supports keyword expressions.
Custom header(s) are present and not empty	Tests for the presence of custom headers and any other headers not included under the standard headers list. .
Custom header(s) contain words	Matches text within any custom headers and other headers not included under the standard headers list. This condition supports keyword expressions.
Email has NO body text	Tests whether the email body contains any text.
Email contains HTML body	Tests if the email includes an HTML body. Emails only having a plain text body fail to match.
Email contains attachments	Tests if email contains any attachments.
Attachment name contains words	Matches keywords within attachment filenames. This condition supports keyword expressions.
Attachment name is exactly/matches filename	Matches either the exact filename or, using the * wildcard, the last part of the filename. The * may only be used at the beginning as follows: *something
Email character set matches words	Matches against the email character set code identified at the MIME headers. This condition supports keyword expressions.
Content media type matches words	Matches against the media types identified at the MIME headers. In MIME encoded emails, attachments and bodies are contained within different parts for which a media type is used to specify the nature of the data held within it. This condition supports keyword expressions.
Sending host matches IPs	Matches against the IP of the host connecting to Exchange for submitting emails. Single IPs, IP ranges and IP/Mask pairs, may be configured for this purpose.

Email size is within range	Matches against the total raw email size. Type supports defining a size range to be matched.
Received time is within range	Matches against the time when the email reaches Exchange. Type supports defining a time range to be matched.
Spam Confidence Level (SCL) is within range	Matches against the SCL value as assigned by the MS Exchange Content Filter before IMF Tune starts its processing. Type supports defining an SCL range to be matched.
SMTP protocol HELO/EHLO command contains words	Matches against the parameters the sending host supplied on issuing the HELO/EHLO command as part of the SMTP protocol session. Legitimate email senders will typically identify a host name that could be used for whitelisting purposes. This condition supports keyword expressions.
SMTP protocol MAIL FROM command contains words	Matches against the sender address specified at the SMTP FROM protocol command. The 'Received from addresses or domains' condition type also tests this sender address (amongst others). However here this condition does not support the * wildcard. Instead it performs a text matching operation supporting keyword expressions.
SMTP protocol RCPT TO command contains words	Matches against the email recipient addresses. This SMTP protocol command gives the list of true recipients an email is addressed to. This may not be the same set of addresses shown at the email client. The 'Sent to recipient addresses or domains' condition type also test this list of addresses. However here this condition does not support the * wildcard. Instead it performs a text matching operation supporting keyword expressions.

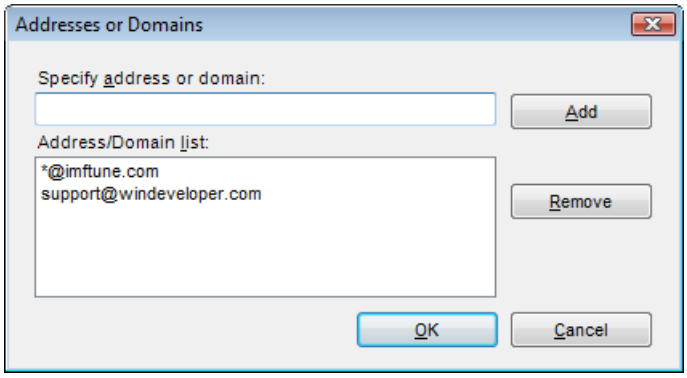
Note: For types supporting keyword expressions see details under Constructing Search Expressions.

4.12.2.2 Address Based Conditions

The condition types ‘Received from addresses or domains’ and ‘Sent to recipient addresses or domains’ support the use of the * wildcard for identifying entire domains. Any of the following formats may be used:

alias@domain
*@domain
@.domain

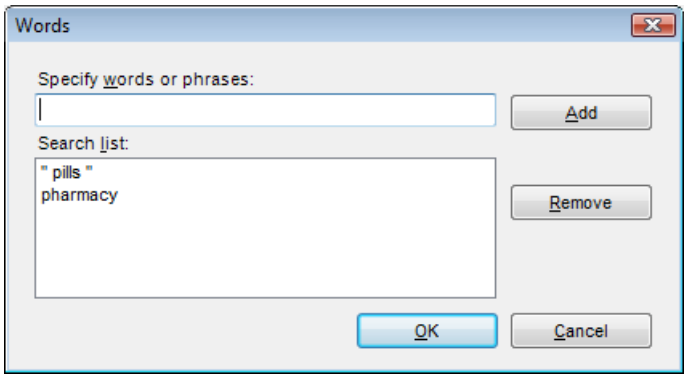
When selecting these condition types, click on the ‘addresses or domains’ link. This brings a list interface to which we can add and remove addresses.



4.12.2.3 Keyword Expression Based Conditions

Most condition types perform a text matching operation supporting keyword expressions. Thus the AND, OR, NOT operators and double quotes have a special meaning.

These conditions include the ‘words’ link in their name. Following the link, brings a list interface where keyword expressions may be entered.

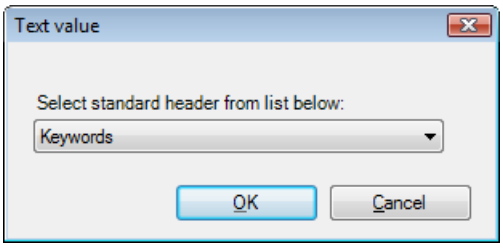


Although supported (for consistency) complicated expressions are normally not necessary when configuring Advanced Rules. Keyword expressions were discussed in detail in Constructing Search Expressions. This section helps appreciating these points:

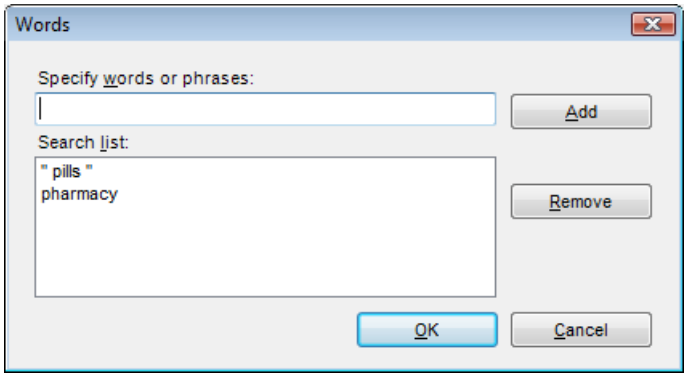
- The AND operator is always implied when entering multiple keywords.
- The effect of the OR operator can be achieved by entering multiple list entries.
- The NOT operator can be avoided by using the Exception list. Keep in mind that exceptions always produce the opposite effect of conditions. Conditions must be matched, whereas exceptions must NOT be matched.

4.12.2.4 Custom/Standard Header Conditions

Configuring conditions for custom and standard headers involve similar steps. Standard headers require choosing a header name from a fixed list. On the other hand, custom headers require typing the name manually.

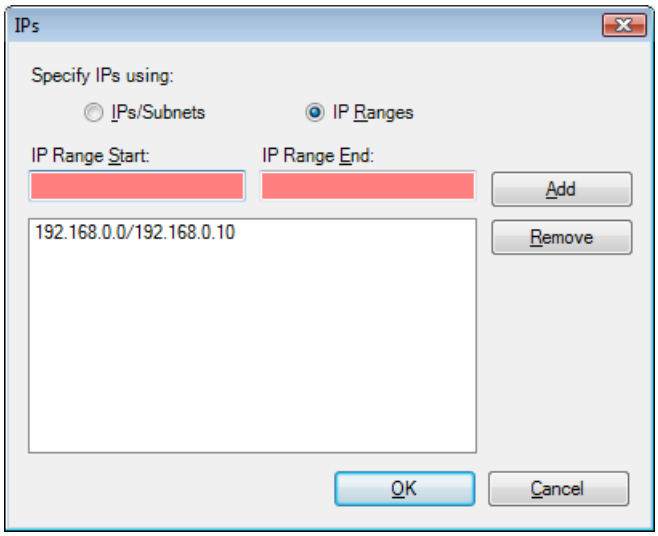


Once the header name is in place, a list interface is available to specify the keyword expressions to be matched against the header value.



4.12.2.5 IP Condition Configuration

Conditions requiring the entry of IPs will have the ‘IPs’ link within their name. Following the link will bring the IP entry list.



To specify a single IP, select IPs/Subnets and enter the IP keeping the default subnet mask to 255.255.255.255. Changing the subnet mask effectively defines a set of IPs matching the IP/Mask pair.

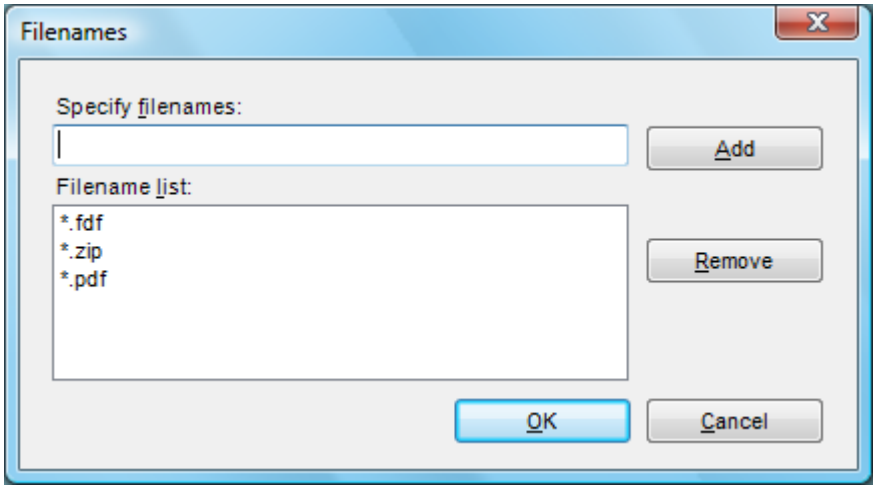
To specify a range, select IP Ranges and enter the lower and upper IP range limits.

4.12.2.6 Filename Based Conditions

The condition type ‘Attachment name is exactly/matches filename’ supports the use of the * wildcard for identifying filenames ending with a common extension. Any of the following formats may be used:

FullFilename.ext
*.ext
*something

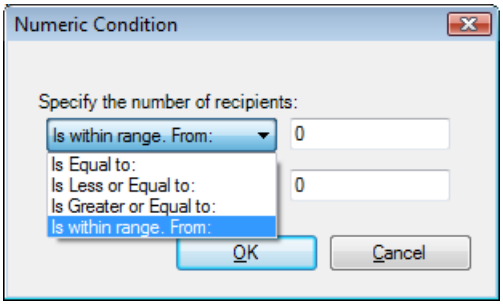
When selecting this condition type, click on the ‘filename’ link. This brings a list interface to which we can add and remove filenames.



Note: This discussion does not apply to the condition ‘Attachment name contains words’. This condition takes regular keyword expressions as discussed in Keyword Expression Based Conditions.

4.12.2.7 Range Based Conditions

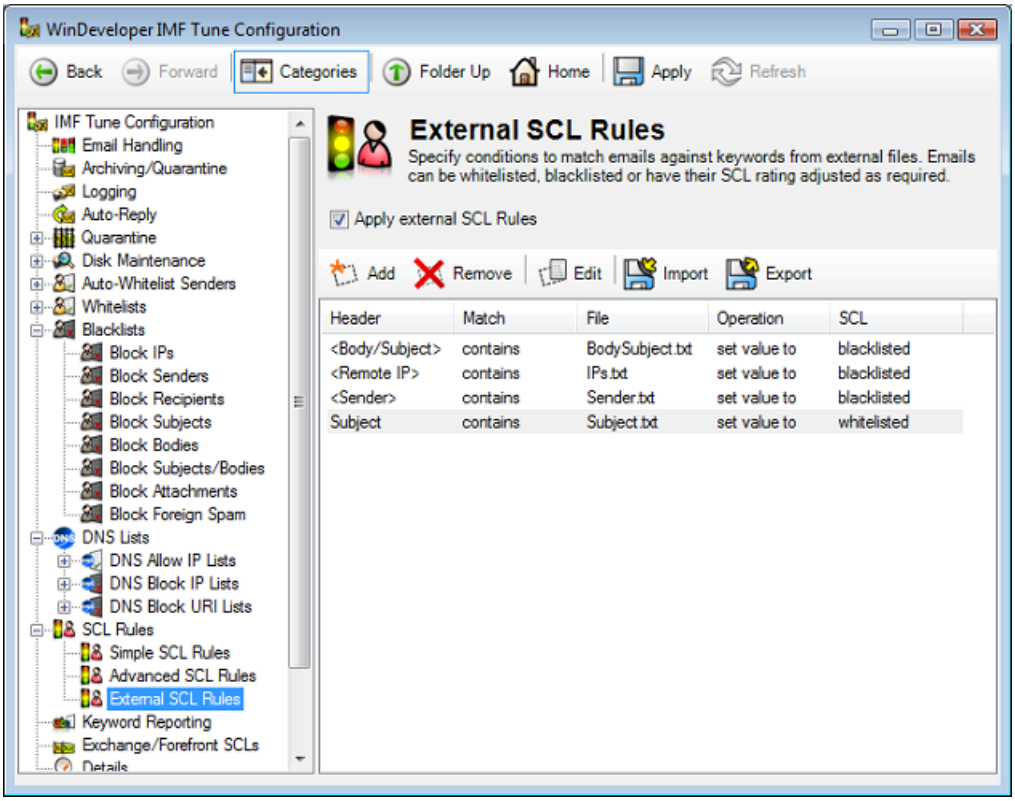
Whenever configuring conditions involving numeric or temporal (time based) value matching, the ability to specify a range is available.



The interface allows us to choose an operator and the upper and lower limits defining the range to be matched.

4.13 External SCL Rules

External SCL Rules provide the opportunity to host rule values in external files.

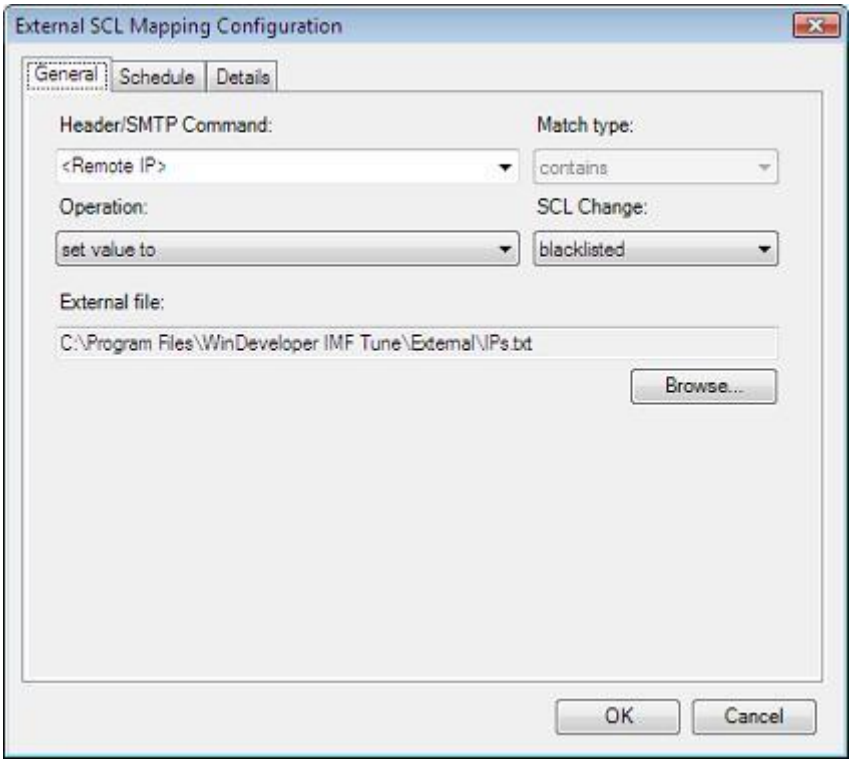


External rules mimic closely the functionality of Simple SCL Rules and have nearly identical interfaces. However these rules will pull the list of keywords, addresses or IPs to be tested against incoming emails, from external files.

Because of the similarities between External and Simple Rules, it is recommended to first review the documentation for Simple SCL Rules before reading through this section. Here we go through the unique characteristics of External SCL Rules.

4.13.1 Working with External SCL Rules

The configuration provides a list interface through which External Rules can be managed. The list interface is identical to the Simple SCL Rules list. Clicking on Add opens the External SCL Mapping configuration dialog.



The dialog is organized in three configuration pages, General, Schedule and Details.

The General page comprises setting for identifying:

1. The email information (IP, address, header or body) the rule is to test.

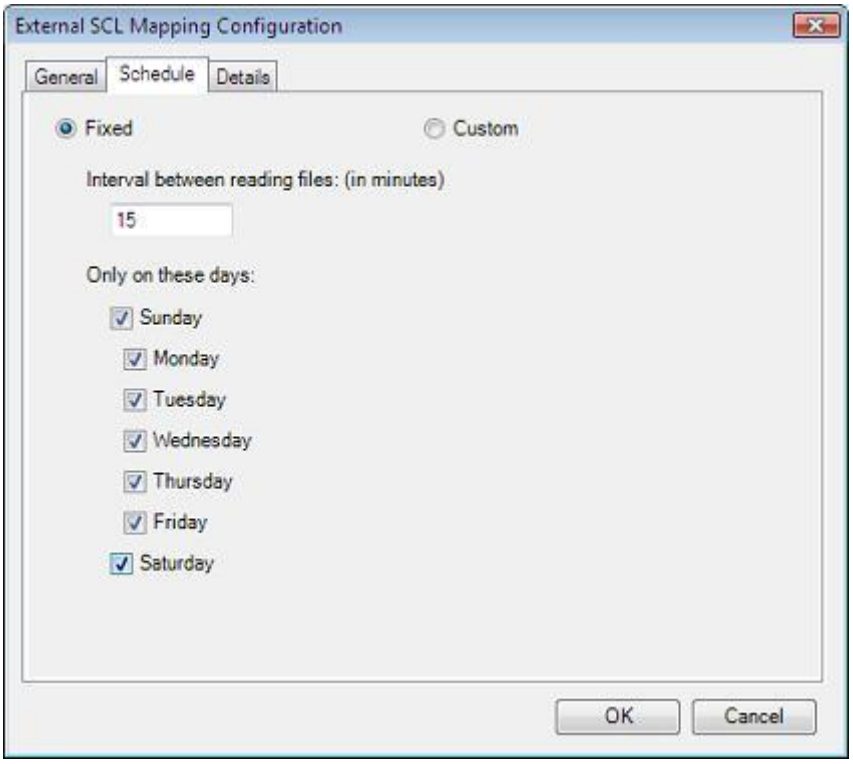
2. The operation to perform on matching an email.

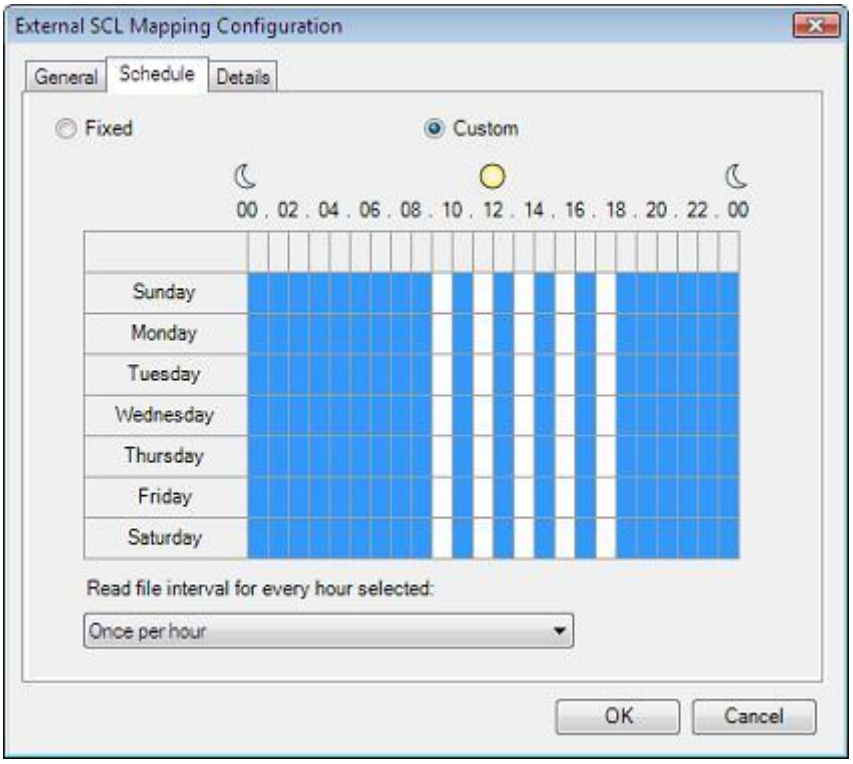
3. The path to an external file containing values to be matched against processed emails.

The interface provides plenty of flexibility. We can setup an External SCL Rule against any standard or custom header, email bodies, sender/recipient addresses or IPs. Through these rules we can choose to whitelist/blacklist emails, set the SCL to any fixed value, or to apply an increment/decrement to the current SCL rating.

Apart for the external file path, the General property page presents the same configuration elements available for Simple SCL Rules. The only difference is that whereas Simple Rules are directly fed with the value to be matched, External Rules are fed with a file path. From here IMF Tune will load the list of values.

External files are processed periodically based on the settings configured at the Schedule property page. IMF Tune supports two types of schedule configuration interfaces, Fixed and Custom.





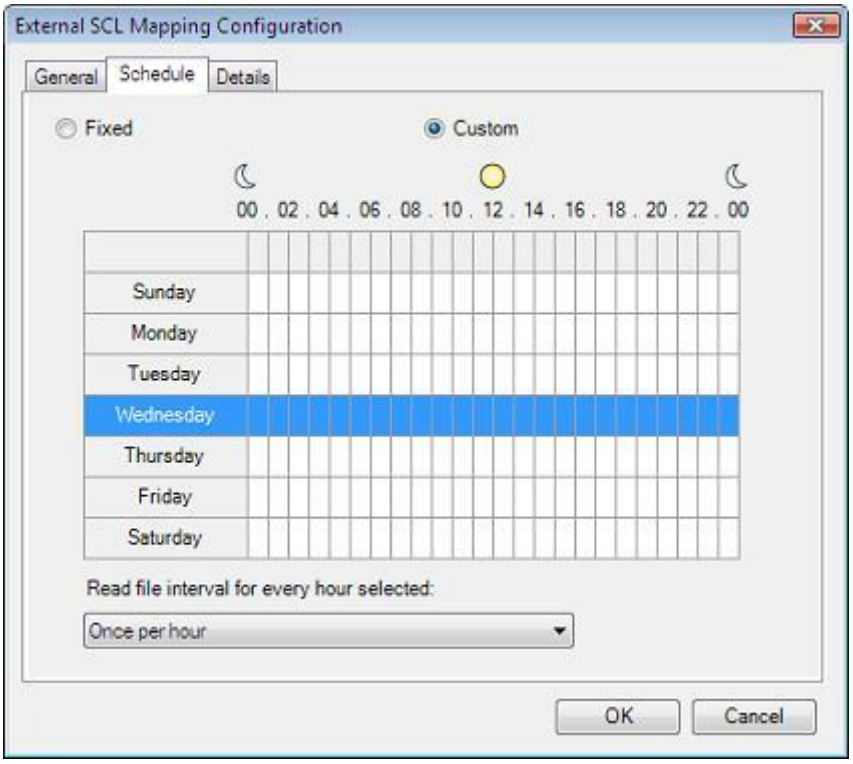
Choose the schedule type from the radio buttons at the top. Switching the schedule type also changes the interface as shown in the above screenshots.

In Fixed Schedule mode, the edit box '*Interval between reading files*' specifies the time between successive file reads. On each time interval, IMF Tune fetches the file and refreshes the rule values. The interval is expressed in minutes and cannot be less than 15.

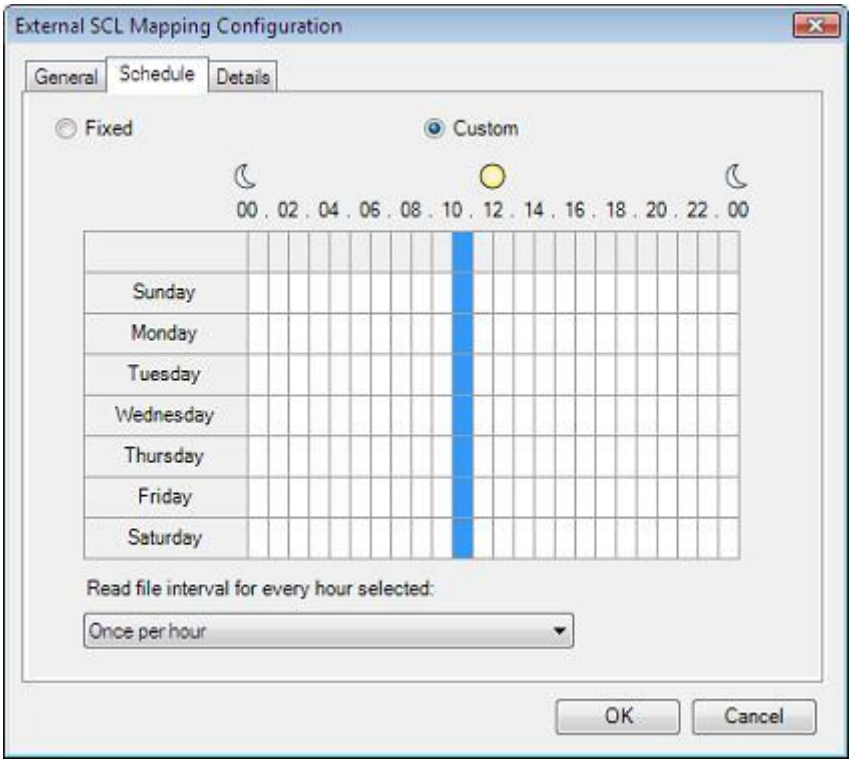
Apart for the interval time, the Fixed Schedule provides seven checkboxes one for each day of the week. IMF Tune only fetches the external file on the days whose checkbox is set.

In Custom Schedule mode, the configuration provides a 24 x 7 matrix interface. The 24 columns represent the hours of the day whereas the 7 rows represent the days of the week. Click the matrix boxes to set/clear individual hours within the schedule. IMF Tune will only read the external file on the selected hours.

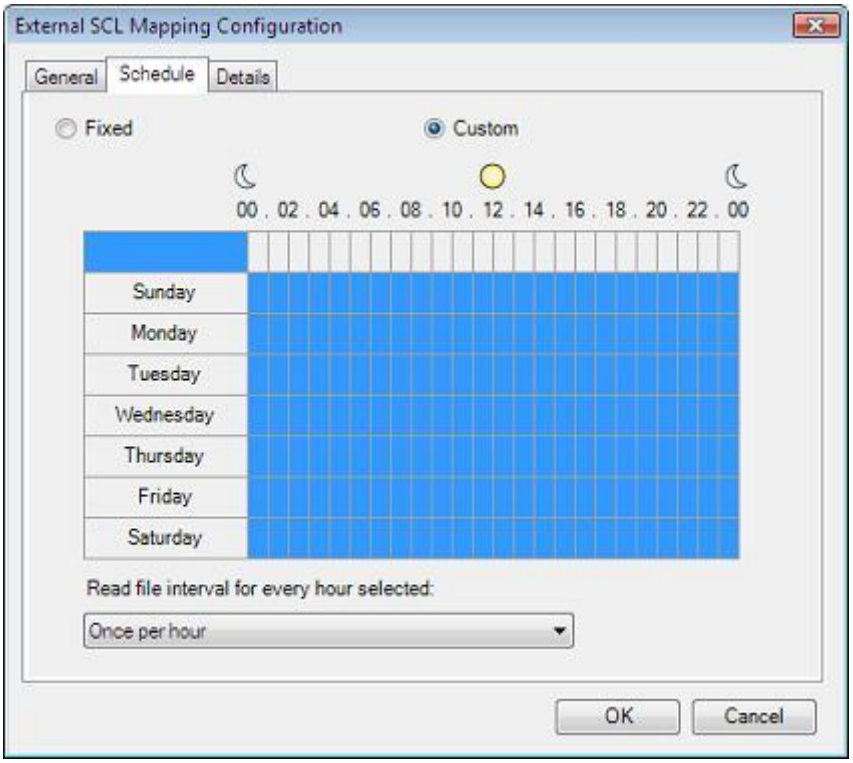
Clicking the boxes in the first Column will set/clear all hours for the selected day.



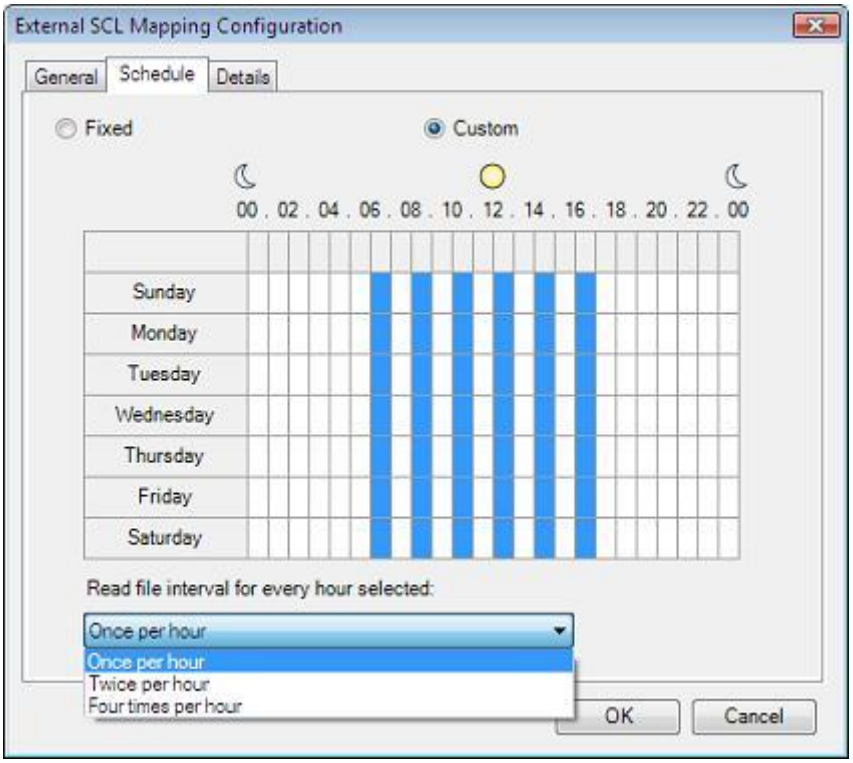
Likewise clicking the boxes in the first row will set/clear an entire column configuring the same hour for all days.



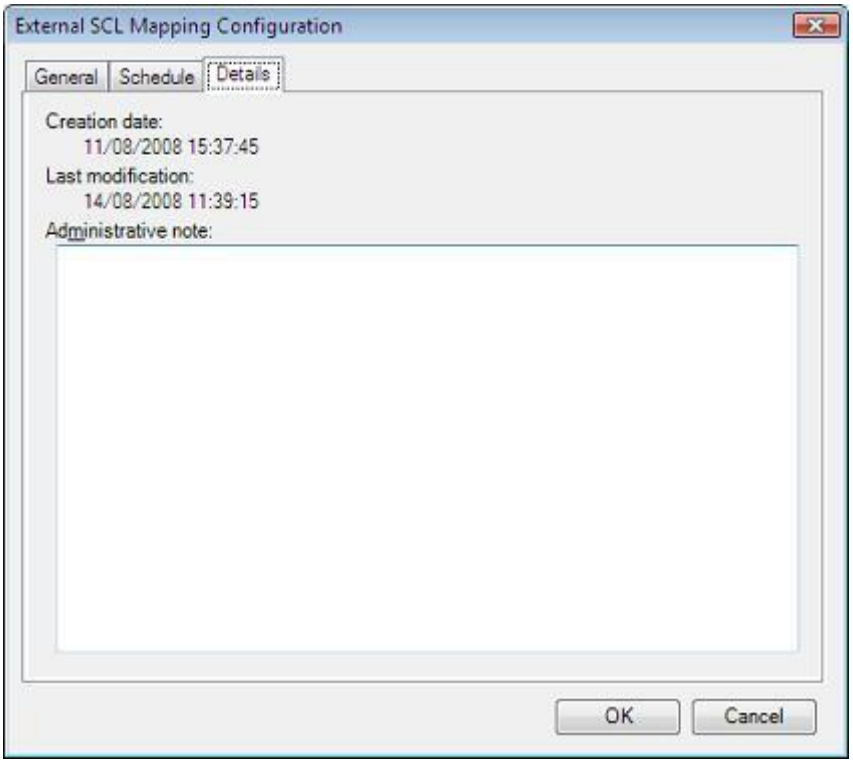
If we click the box at the top left corner we set/clear the entire matrix with one click.



Underneath the Schedule matrix the *'Read file interval for every hour selected'* list provides a selection of how often should the file be refreshed within the selected hours. Here we can choose to refresh the file once, twice or four times an hour.



The External SCL Rules dialog also provides a details page where we can keep track of the creation and last modification times for the rule. Here space is also available for Administrative notes.



4.13.2 External File Format

The External SCL Rules source file must meet the following requirements:

1. The file may be encoded in 7-bit ASCII, UTF-8 or UTF-16. Although two UTF encoding formats are supported, all characters are expected to be within the standard Windows 1252 character set.

2. Multiple values must be separated by a carriage return line feed (CRLF) sequence. For files generated on non-Windows platforms the line feed only separator (LF) is also supported.

Of course depending on the type of rule being setup, file entries will also have additional format requirements. For example an IP rule will only accept entries in one of these formats:
xxx.xxx.xxx.xxx – single IPs
xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy – IP range
Xxx.xxx.xxx.xxx (yyy.yyy.yyy.yyy) – IP/subnet pair

A rule being applied against sender or recipient addresses will expect address in the format something@something, *@something or *@*.something. Likewise a rule applied to an email header or body supports the expression syntax including the use of AND OR NOT operators and double quotes.

The type of values an external file is expected to contain depends on the '*Header/SMTP Command'* setting configured at the Rule General Property page. This setting is documented exhaustively at the Simple SCL Rules documentation.

The file format is identical to that supported by the white/black list import/export functionality. So it can be useful to export values from these lists for an example of a correctly formatted file.

NOTE: Whenever IMF Tune processes external files, its entries undergo a validation process. Any invalid entries will be silently ignored.

4.13.3 External File UNC Path

External Rule files may be placed on a shared drive to facilitate access from different machines. In this case the rule is configured with the UNC file path in the format:
\\<machine name>\<share name>\<any directories>\<filename>

This is especially useful when running IMF Tune on more than one machine. At IMF Tune we then configure External Rules to pull the keywords from this central file. In many cases this eliminates the need to replicate configuration settings from one machine to another.

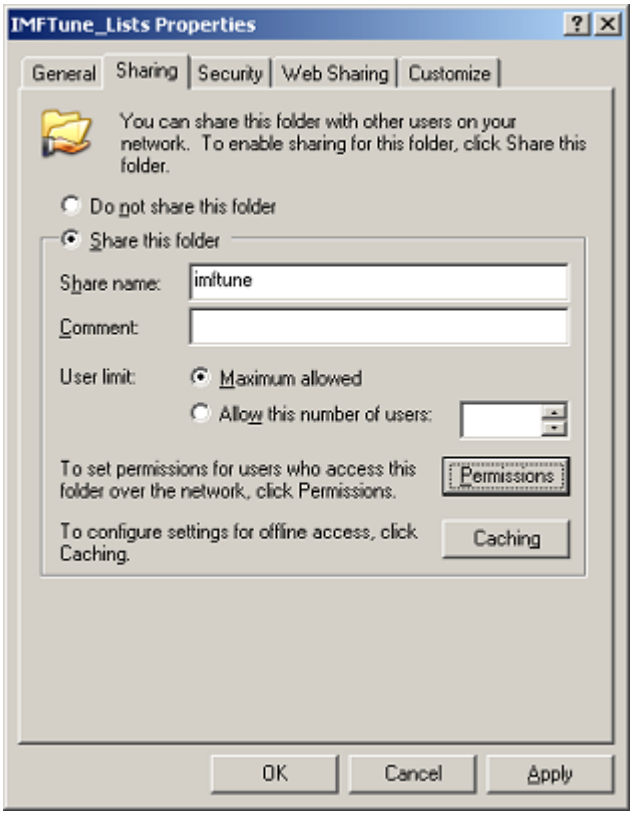
4.13.4 External File Access Permissions

When using External Rules it is important to ensure that IMF Tune is able to read the file being configured.

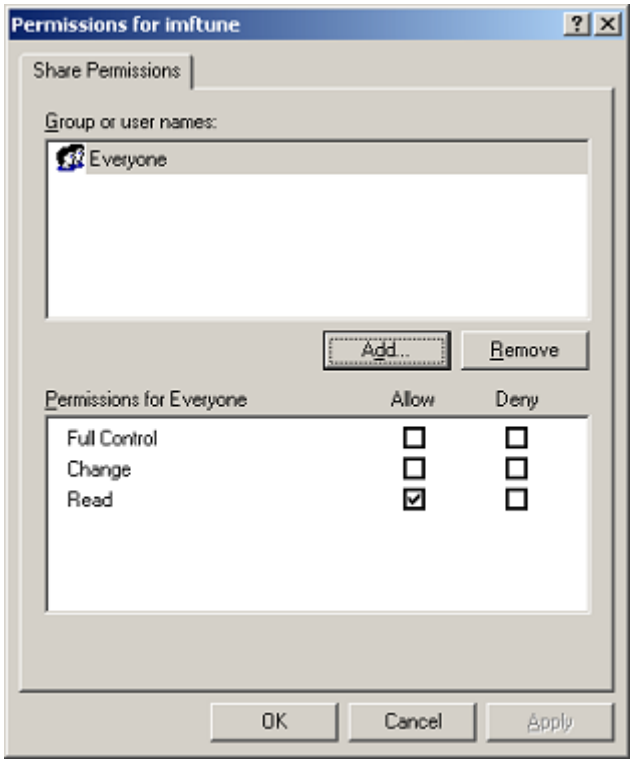
The IMF Tune Attendant service is the process responsible for fetching these files. This service runs under the LocalSystem account. Thus when configuring any permissions these have to be assigned to the Exchange Server Active Directory machine object.

The following steps show how to configure the necessary permissions on a network share. However the important point to appreciate is the fact that permissions are being assigned to the Exchange server machine object. Similar steps would be followed when assigning NTFS permissions on local drives.

1. In Windows Explorer locate the directory to be shared.
2. Open the directory properties (Right-Click | Properties)
3. Select the Sharing Property Page
4. Select 'Share this folder' and set the share name



5. Click on the Permissions button.



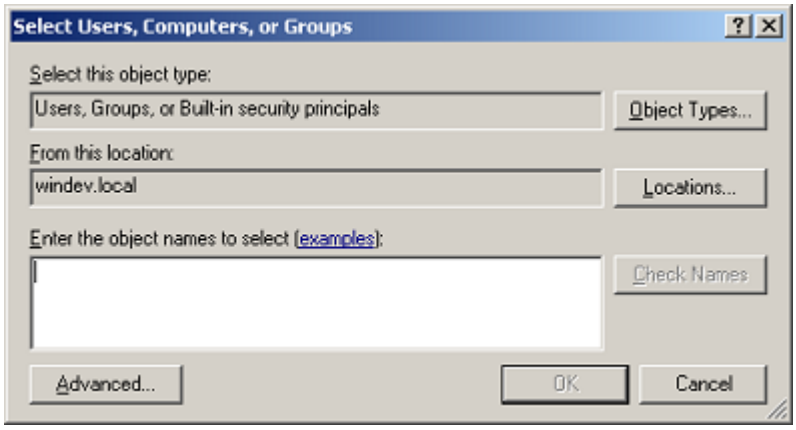
By default Everyone is given the Read permission. This should be enough for IMF Tune to work.

However if you want to limit access on this share you can remove this entry and specifically assign the Read permission to the Exchange server on which IMF Tune is running.

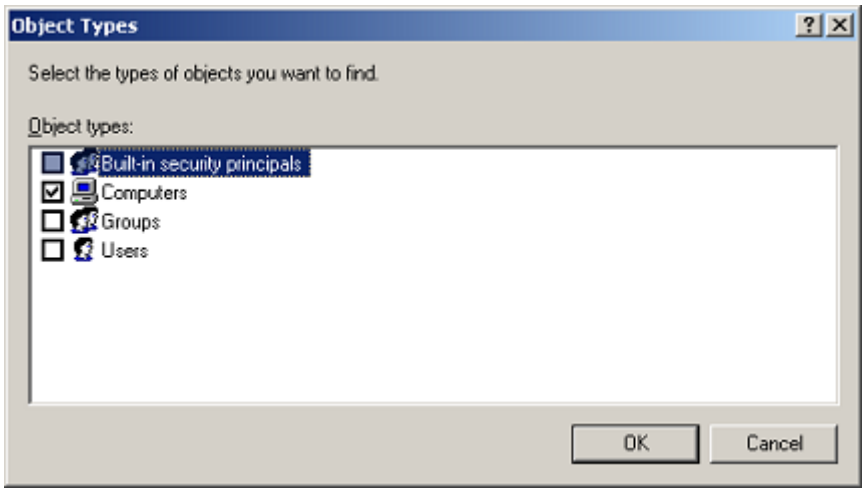
NOTE: IMF Tune uses the 'IMF Tune Attendant' service to read External SCL Rule files. This means that in order for IMF Tune to be assigned rights over network resources the machine account must be used.

Windows creates an AD object for each computer within a network. The computer object for the Exchange server on which IMF Tune is running should be identifiable using the computer name. In the steps that follow we see how to assign the rights to an Exchange server named ExServer.

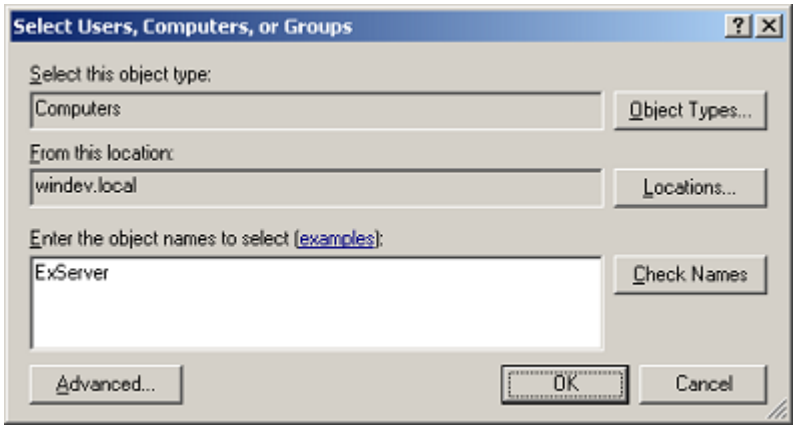
6. Click Add to choose the Exchange server AD object.



7. Click on 'Object Types' button and set the checkbox for Computers. All other checkboxes may be cleared in this case. When ready click OK to complete object type selection.



8. Enter the Exchange server name at the bottom and click OK.



9. The Exchange Server object should now be in your Permissions list. IMF Tune will only require Read access.

10. Save changes to complete the configuration.

4.14 Constructing Search Expressions

The IMF Tune configuration supports advanced keyword expressions. These may be used in Subject, Body and Subject/Body white/black lists. Furthermore expressions are also supported in SCL Rules.

An expression is composed of one or more keywords/phrases. These are combined together with the use of the AND, OR, NOT operators. In this manner complex expressions may be constructed so as to better identify the matching criteria.

Expressions also support the use of double quotes. This enables combining multiple keywords into a single phrase. It also forces handling the phrase literally, as we shall see later.

In general, constructing expressions should be fairly intuitive. Furthermore the configuration provides the Expression Builder. This takes care to construct well-formed expressions with minimal effort. Nevertheless it is sometimes useful to understand the rules behind valid expressions as it helps us construct more effective email filtering rules.

4.14.1 Basic Expression Syntax

The simplest form of expression is one composed of a set of keywords separated by white space such as:
original replica watch

Looking at this expression we can already identify some important characteristics:

1. Number of keywords
   This expression is composed of three keywords. Each of these must be matched against the email information in order for the entire expression to be matched.

2. Position of keywords
   The keyword order is not relevant. Emails containing the keywords in any order would still match the expression:
   original watch replica
   replica watch original

   Keywords will also be matched in case these are separated by other text or punctuation. Again IMF Tune only requires the presence of the three keywords. Example:
   *Get your **replica watch** now. Same as the **original**!*

3. Case Sensitivity
   Matching is never case sensitive. The expression will also match:
   ORIGINAL RepLicA watch

4. Whole Word Matching
   The keywords will also match sub-strings such as:
   *The **original** footage was **replica**ted and **watch**ed various times.*

4.14.2 Exact Matching

IMF Tune gives special meaning to double quotes. These are used to group keywords into one phrase and instruct IMF Tune to handle the enclosed text literally. Consider this expression:
“original replica” watch

This is the same expression considered in the previous section, except for the introduction of double quotes. The expression is now processed as follows:

1. Number of keywords
   This expression is composed of two elements “original replica” and “watch”.

2. Position of keywords
   Since “original replica” is now one phrase, IMF Tune will only match this when found in that exact order. On the other hand “watch” may appear anywhere. Example:
   Watch*-out for this* ***original replica***

3. Case Sensitivity
   Matching is always case insensitive even when double quotes are used. Thus the expression will also match:
   Watch*-out for this* ***Original REPLICA***

4. Whole Word Matching
   Despite the use of double quotes, the phrase may match other words with similar spelling such as::
   Watch *Ab****original Replica****s*

4.14.3 Whole Word, Word Start/End Matching

In the Exact Matching section we have seen how the phrase “original replica” matched “Aboriginal Replicas”. The double quotes here only enforced literal matching but did not exclude sub-string matching.

In order to exclude such a match the expression must be changed as follows:
“ original replica ” watches

Here we inserted a white space between the double quotes and the first and last characters. The phrase now will only match whole words.

The same logic may be used to match words starting or ending with specific text. For example here the keyword is enclosed by double quotes and the leading quote is followed by a white space:
“ watch”

This will match each of these words:
Watch*es*
Watch*er*
Watch*ing*

On the other hand, in the next example IMF Tune will only match words ending with the text “watch”. The expression here contains a white space preceding the closing quote.
“watch ”

This will match each of these words:
*Bay****watch***
*Stop****watch***

4.14.4 Punctuation Handling

When discussing whole word matching, white space was considered as the delimiter identifying the word boundaries. Nevertheless words are also very often separated by punctuation. For this reason IMF Tune also allows whole words to be surrounded by punctuation. Specifically the following punctuation marks are allowed:

: ; , . ? !

Consider a phrase requiring whole word matching such as:
“ watch ”

This would successfully match all of these:
*Original replica **watch**!*
*Replica **watch**, get yours now!*

Indeed the phrase will match any combination of surrounding punctuation including less meaningful ones:
*!**watch**…*
*;**watch**!*
*?**watch**;*

4.14.5 Minimum Keyword Length

IMF Tune supports expression processing against email headers and bodies. Apart for one exception, the same expression syntax rules apply in all cases. The only difference is the minimum keyword length. Keywords to be matched against email bodies must be at least 3 characters in length.

In general email bodies are made up of long text runs. Any short keyword is likely to lead to unexpected matches. Thus when matching body information extra care is required and this limit is intended to alert administrators against keywords of this type.

On the other hand email headers are normally much shorter in length. Thus the risk of unexpected matches is lower and no minimum limit is imposed.

4.14.6 AND OR NOT Operators

In the previous sections we looked at expressions composed of keywords/phrases separated by white space. Each of these had to be matched in order for the entire expression to be matched.

IMF Tune also supports the use of the AND, OR, NOT operators. These change the matching requirements for the keywords on which they operate. The following summarizes the behavior of each operator:

AND – Combines keywords that must be matched (unless the NOT operator is in use). It joins the two keywords on each side of the operator. Indeed this is the default behavior. Keywords separated by just a white space are also assumed to be combined in this manner. Thus even though AND has a special meaning to IMF Tune, it may be simply replaced by a white space. All of the following expressions are equivalent:

Original Replica Watch
Original AND Replica AND Watch
Original Replica AND Watch

OR – Combines a set of keywords out of which at least one must be matched. Again this joins the keywords on each side of the operator. Here are some examples of keywords combined in this manner:

pharmacy OR pharmacies OR pharmaceutical
pills OR pi11s OR pill2

NOT – Identifies keywords that must not be matched. This acts on the keyword immediately following the operator. For example IMF stands for Intelligent Message Filter. It may also stand for International Monetary Fund. So I could specify one of these to match IMF but not International Monetary Fund:

IMF NOT International NOT Monetary NOT Fund
IMF NOT "International Monetary Fund"

Note that the above two expressions are not equivalent.

IMF Tune expression processing is completely case insensitive. This is true also for operators that may be written in any upper/lower case combination.

Within an expression keywords can be re-ordered without changing the meaning. In general what is most important is to keep any set of ORed keywords side-by-side. The following expressions are equivalent. Note how we changed the keyword order and dropped the AND (which is the default operator).

Pills OR pi11s AND pharmacy OR pharmaceutical OR ph@rm@cy
Pharmacy OR ph@rm@cy OR pharmaceutical Pills OR pi11s

IMF Tune whenever meeting the operators will automatically handle these as special expression elements. Sometimes we may need to match these as literal text. In this case just enclose the keyword in double quotes as shown below:

Exchange "and" Sharepoint Newsletter
one, two "or" three

4.14.7 Invalid and Illegal Operator Sequences

The AND, OR, NOT operators are meant to combine keywords to construct more advanced expressions. Nevertheless there exists many ways how these operators may be used incorrectly.

Some operator sequences are invalid by definition. For example, the NOT operator acts upon the keyword that follows. Thus a NOT operator may never be followed by any other operator.

Similarly the AND, OR operators are meant to combine two keywords. Thus these may never appear next to each other.

It is ok to have AND followed by a NOT operator such as:
IMF AND NOT Monetary

Nevertheless it is illegal (not invalid) to have an expression entirely composed of NOTed keywords such as:
NOT International NOT Monetary NOT Fund

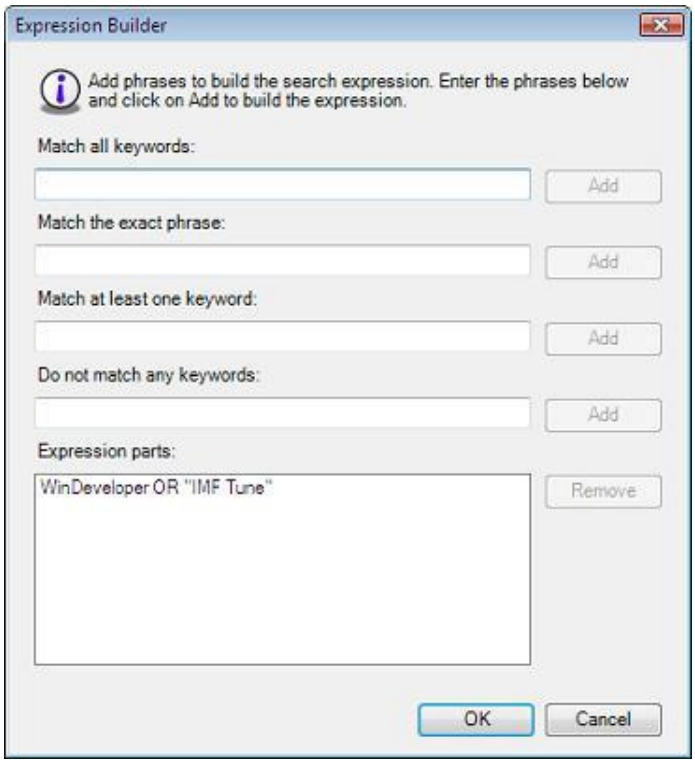
Although the above is a valid expression, it is deemed to be illegal as it would lead many matches. Indeed such expressions would match almost all emails.

Similarly the NOT operator may not be used in combination with the OR operator. Again this causes the ORed set to match most emails. Here are some examples of illegal expressions:
IMF OR NOT Monetary
NOT Monetary OR IMF

The above two expressions are equivalent. Both are illegal since NOT Monetary would cause many matches.

4.14.8 Working with the Expression Builder

Constructing Search Expressions described the rules for composing valid keyword expressions. IMF Tune provides a much simpler alternative to remembering these details. This is the Expression Builder, an interface through which complex expressions may be constructed.



The dialog provides for entering four different types of keywords/phrases as summarized below.

Match all keywords	Enter a set of keywords separated by white space. Each of these keywords must be found in order for the Expression to be matched. Keywords may be matched in any order when compared against the email content.
Match the exact phrase	Enter a phrase composed of any number of words to be matched literally and in the exact order specified.
Match at least one keyword	Enter a set of keywords separated by white space. At least one of these must be found in order for the Expression to be matched. For example in a blacklist we could specify different ways for spelling ‘pharmacy’ in order to match this category of spam.

Do not match any keywords	Enter a set of keywords separated by white space. The Expression will only be matched if none of these keywords are found.

In order to construct the expression, fill in any of the edit boxes and click on the adjacent Add button. This will automatically validate and transfer the keywords to the Expression Parts list at the bottom. Here the order of the individual expression parts is not relevant.

To add multiple phrases into the same expression, just enter the keywords in the appropriate edit box, click on Add, and repeat the procedure as necessary.

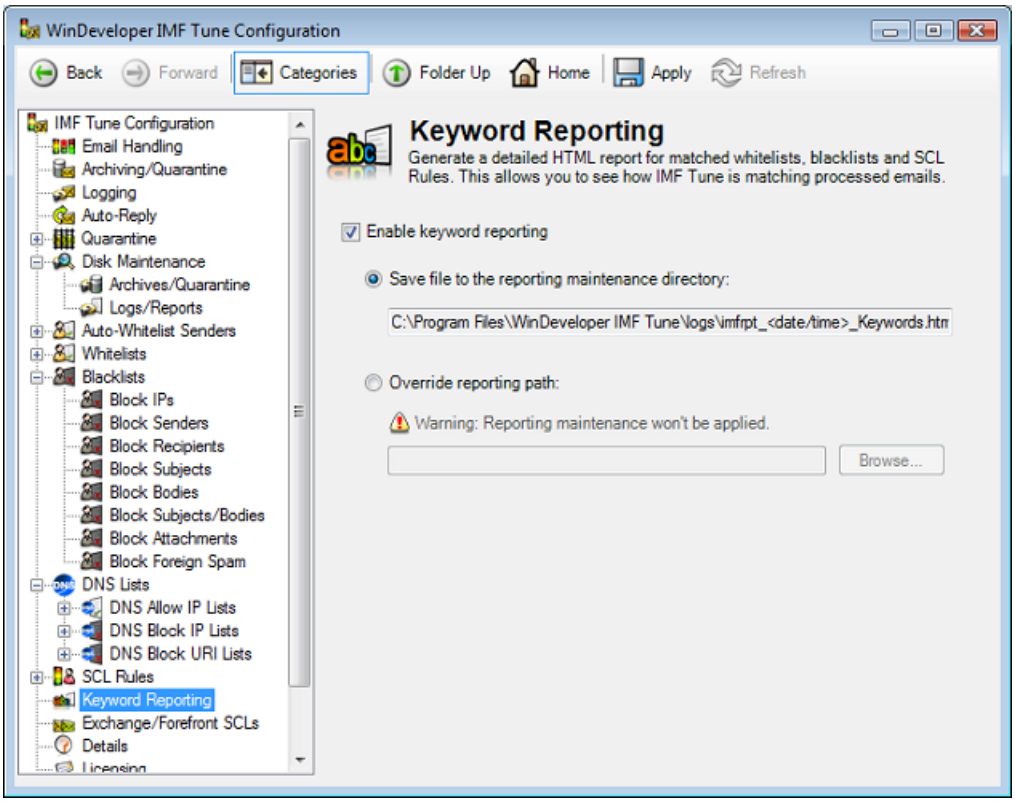
To delete any of the Expression Parts just select it and click on the Remove button.

Once all necessary keywords are entered and added, click on OK to save the expression.

4.15 Keyword Reporting

Keyword Reporting allows us to see how emails are matching the various IMF Tune filtering srages. An HTML formatted report is generated that is especially useful when verifying the effectiveness of our current configuration. If we are uncertain why an email was white/black listed or whether an SCL rule is only matching the intended class of emails, then this is the report to look at.

Configuring Keyword Reporting is a trivial matter. We just enable it and specify the location for the report file under the Keyword Reporting category.



Just like for Email Logging, selecting ‘Save File to the Reporting Maintenance Directory’, will allow Disk Maintenance to automatically manage, backup and purge these report files.

Otherwise we can go for any other local disk location by selecting ‘Override Reporting Path’. However in this case we lose the Disk Maintenance functionality.

Once enabled, IMF Tune will start reporting on each email matching some filtering rule. Emails that don’t trigger any filter won’t show up in this report. This is how the report looks like:

WinDeveloper IMF Tune - Keyword Reporting - Windows Internet Explorer
Google
Favorites
WinDeveloper IMF Tune - Keyword Reporting
WinDeveloper IMF Tune - Keyword Reporting
From <spam@testing.local> Date/Time 5/21/2010 14:12:08
To <user1@horizon.local>
Subject Over 1,500,000 bottles sold, Safe & Effective PenisEnlargement Herbal Pills rpchk
Initial SCL 8
Final SCL 9
Matches 1
Header Expression Source
subject " pills " ...rgement Herbal Pills rpchk
Operation increment SCL by 1
From <spam@testing.local> Date/Time 5/21/2010 14:12:11
To <user1@horizon.local>
Subject Please complete your application Mon, 19 Mar 2010 08:15:44 -0800
Initial SCL 5
Final SCL 6
Matches 1
Header Expression Source
Body/Subject mortgage OR "home loan" ...do Hancock Bay Home Loans In any free
Operation set SCL to 6

4.15.1 Understanding the Keyword Report

The Keyword Report file contains all the necessary information for us to understand why and how an email triggered a match.

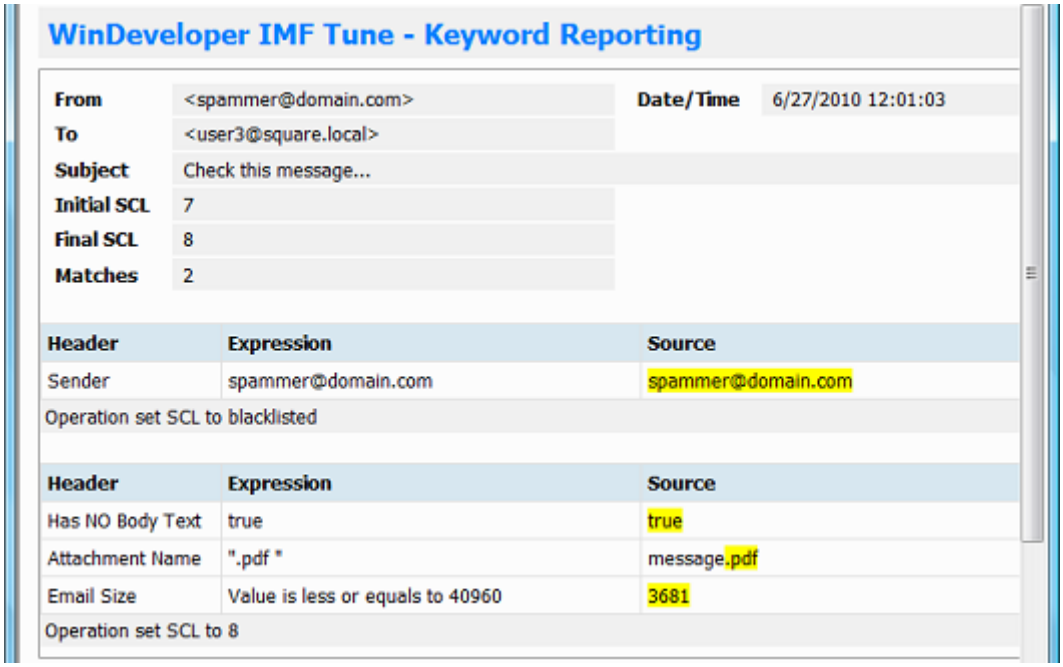
If an SCL Rule was composed of multiple conditions, then the report will show how each of the individual conditions was matched. Furthermore if an email matches more than one rule or matches a mix of rules and white/black lists then again the report will highlight each individual match that was involved.

The above sample shows a report for two different emails. For each email the report is composed of a header area with general information and a tabular body illustrating how the email was matched.

The following table describes the fields presented at the report header area:

Field Name	Description
Date/Time	The date and time when IMF Tune processed the email.
From	The email From header. This is the sender information shown at the email client.
To	The email To header. This is the set of To recipients shown at the email client. Note that these may not be the true or complete list of recipients to which the email was addressed.
Subject	The email subject.
Initial SCL	The SCL value assigned by the Exchange Content Filter/Intelligent Message Filter/Forefront before IMF Tune starts processing.
Final SCL	The final SCL value that resulted after IMF Tune completes its filtering.
Matches	The total number of matches the email triggered. If an email matches the same white/black list multiple times, this is only counted once.

The Report body area is composed of a sequence of tables, one for each match. In the following sample we see a report for an email that matched both a sender blacklist and an SCL Advanced Rule (composed of 3 conditions).



WinDeveloper IMF Tune - Keyword Reporting

From	<spammer@domain.com>	**Date/Time**	6/27/2010 12:01:03
To	<user3@square.local>		
Subject	Check this message...		
Initial SCL	7		
Final SCL	8		
Matches	2		

Header	Expression	Source
Sender	spammer@domain.com	spammer@domain.com
Operation set SCL to blacklisted		

Header	Expression	Source
Has NO Body Text	true	true
Attachment Name	".pdf "	message.pdf
Email Size	Value is less or equals to 40960	3681
Operation set SCL to 8		

The table is formed of three main columns that describe individual matches. An Advanced Rule composed of multiple conditions will have one row for each. At the bottom a final row shows the type of action this match has triggered. It is important to note how the 'Final SCL' shown at the report header area is the result of the Initial SCL and the individual actions triggered by each match.

The following is a description of the report body columns:

Column Name	Description
Header	The type of email information that was matched. This may be an email header, but may also be an IP, SMTP Protocol Data or other computed email information.
Expression	The white/black list entry, Rule condition value or DNS list that was matched. This may be a keyword expression, an email address or domain, an IP, an email size, or any type of configuration element that IMF Tune allows for identifying the information to be matched.
Source	The source email data that was actually matched. If for example a subject blacklist is matched, here we see part of the email subject highlighting the exact text sequence that triggered the match.

4.16 Exchange/Forefront SCLs (Exchange 2007/2010/2013)

The **Exchange/Forefront SCLs** category is especially useful when running IMF Tune with Forefront Protection 2010 for Exchange. From here you configure how IMF Tune is to deal with emails having an initial SCL -1 rating.

IMF Tune processes emails after that the Exchange IMF/Content Filter/Forefront completes its own processing. So IMF Tune starts from an initial SCL that can be anything from -1 to 9.

Exchange 2003 IMF and Exchange 2007/2010/2013 Content Filter assign SCL -1 only when an email matches a whitelist or in case of internal emails. Note that here we are referring to Exchange whitelists not IMF Tune whitelists. For example Exchange provides the IP Accept List. If an email is received from a host whose IP matches this Accept List an SCL -1 rating is assigned.

Forefront assigns SCL -1 with less restraint. Indeed, it uses SCL -1 to also stamp emails classified as legitimate by the Forefront Content Filter. This is the case even if the email does not match any whitelist.

The distinction between whitelisted emails and emails classified as legitimate through content analysis is useful to IMF Tune. When IMF Tune finds a whitelisted email (SCL -1), no blacklists or SCL Rules are applied. So with Forefront's rating system we end up with many more emails bypassing blacklist processing.

Let's say our Organization wants to blacklist a mailing list that sends out daily jokes. This is an opt-in mailing and Forefront correctly classifies these emails as legitimate assigning SCL -1. The IMF Tune blacklists will be bypassed unless we change the settings at the **Exchange/Forefront SCLs** category.

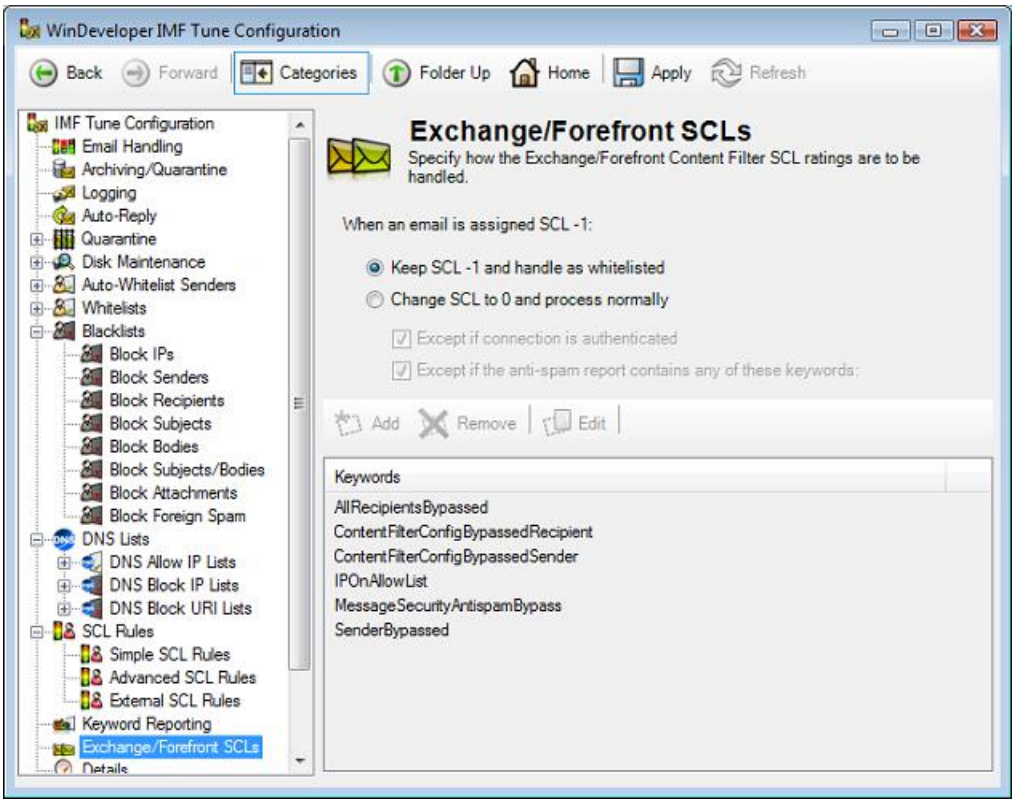
4.16.1 Customizing SCL -1 Handling

IMF Tune can be configured to further analyze emails having an SCL -1 rating. Normally the goal is to distinguish between emails that are explicitly whitelisted and emails classified as legitimate by Forefront content filtering.

IMF Tune does this by looking for special keywords within the header:
X-MS-Exchange-Organization-Antispam-Report

This header gives details on how the SCL rating was arrived at. For example if an email matches the Exchange IP Allow List, the report will contain the keyword **IPOnAllowList**. Other keywords are used to identify other Exchange built-in whitelists.

To enable this functionality go to the **Exchange/Forefront SCLs** category.



By default IMF Tune is configured with:
Keep SCL -1 and handle as whitelisted

In this mode IMF Tune won't apply any blacklists and SCL rules to emails having an SCL -1 rating. This is the correct behaviour when employing the built-in Exchange 2007/2010/2013 Content Filter.

When running Forefront we may want to change this setting to:
Change SCL to 0 and process normally

With this setting IMF Tune is allowed to change the initial rating from -1 to 0. IMF Tune is then able to process the email normally applying whitelists, blacklists and rules to reach the final SCL rating.

This change in SCL is not done blindly. The process is controlled through a set of configurable exceptions that are enabled through the checkboxes:
Except if connection is authenticated
Except if the anti-spam report contains any of these keywords

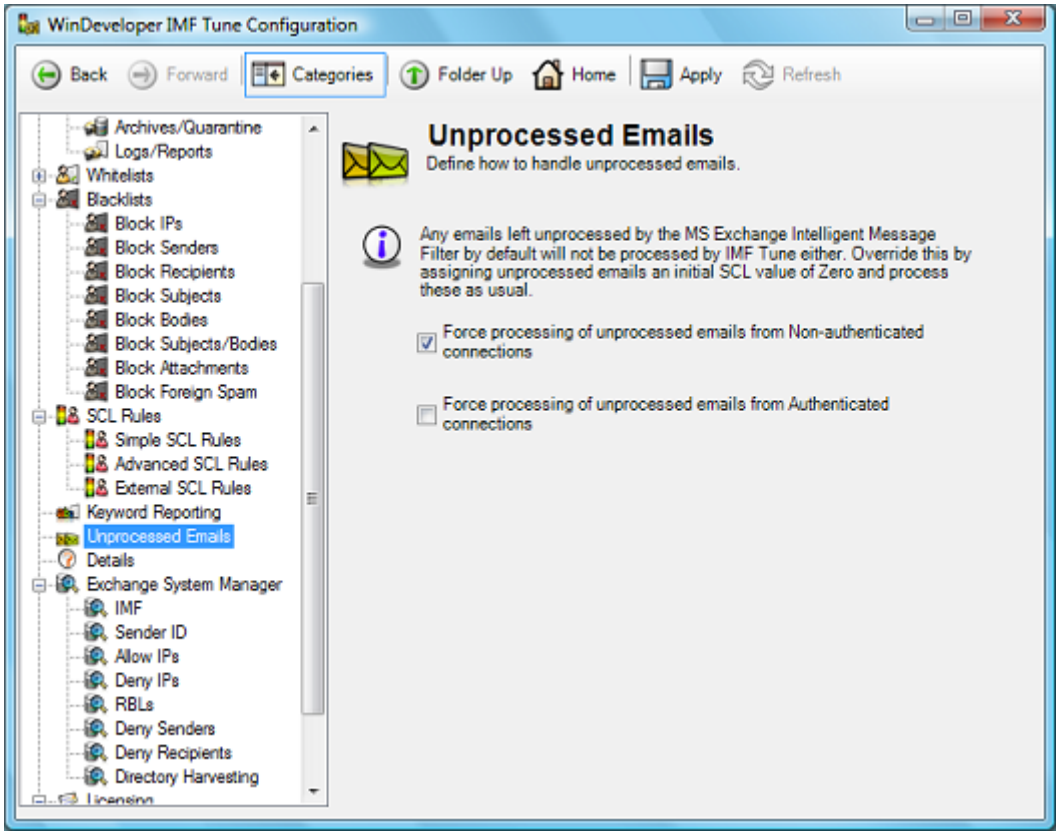
Following these checkboxes, we have the keyword list to be tested against the anti-spam report header. This is initialized with a set of standard keywords obtained from official documentation and through testing. Thus WinDeveloper recommends caution when modifying this list.

4.17 Unprocessed Emails (Exchange 2003 Only)

IMF Tune is tightly integrated with the MS Intelligent Message Filter. Amongst other things, this means that IMF Tune only processes emails that the MS IMF itself processes. If for whatever reason IMF skips email processing, IMF Tune classifies this as unprocessed. In that case white/black lists and SCL Rules are not applied.

This behavior can be overridden from the configuration Unprocessed Emails category. IMF Tune can be instructed to assign an initial SCL value of zero to unprocessed emails and to apply white/black lists and SCL Rules as usual.

Handling of unprocessed emails can be enabled for un-authenticated (anonymous) and/or authenticated connections through separate checkboxes.



The MS IMF does not process emails larger than 3Mb. Through this functionality IMF Tune could be forced to still process these emails.

In the same manner, IMF Tune could even be employed when the MS IMF is disabled altogether. This is sometimes useful when running other anti-spam filters in front of Exchange. Some examples include dedicated anti-spam appliances or external anti-spam service providers. In this case IMF Tune could be just employed for its Exchange Integration functionality without involving the MS IMF as an extra filtering layer.

4.18 Exchange System Manager Anti-Spam Settings (Exchange 2003 Only)

The Exchange System Manager IMF Tune configuration category exposes key anti-spam settings as configured at the Exchange management console. This category is only available in IMF Tune for Exchange 2003. It includes the Exchange Intelligent Message Filter settings and the various Exchange 2003 options for sender id, connection, sender and recipient filtering. IMF Tune gives read only access to these settings and any changes must still be done through the Exchange Management console.

Once IMF Tune is installed we effectively have three anti-spam processing layers. Firstly we have Exchange 2003 sender id, connection, sender and recipient filtering; secondly we have IMF and finally IMF Tune. Bringing all settings into a single dedicated interface enables the administrator to more effectively visualize the overall system setup.

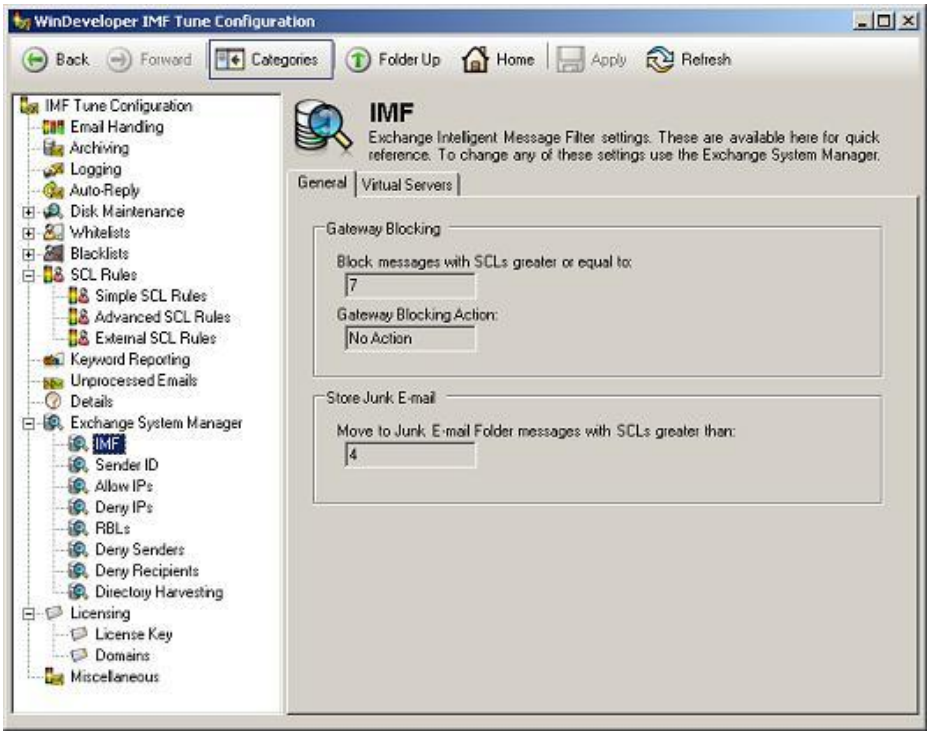
From the feedback received at WinDeveloper, it is clear there is lack of awareness of the functionality readily available from Exchange. IMF Tune organizes the Exchange settings in a different way from that presented by the ESM. It breaks down the various Exchange settings in order to better highlight each of the available features. As an example the IP allow and deny lists; are separated from the RBL configuration.

Another issue typically causing confusion is the enablement of the various anti-spam protection options. The ESM presents this functionality at the virtual server configuration, rather than together with the filtering lists. Furthermore the enablement settings differ depending on the Exchange SP level. IMF Tune presents the list of virtual server for each feature side-by-side. This immediately clarifies the enablement status.

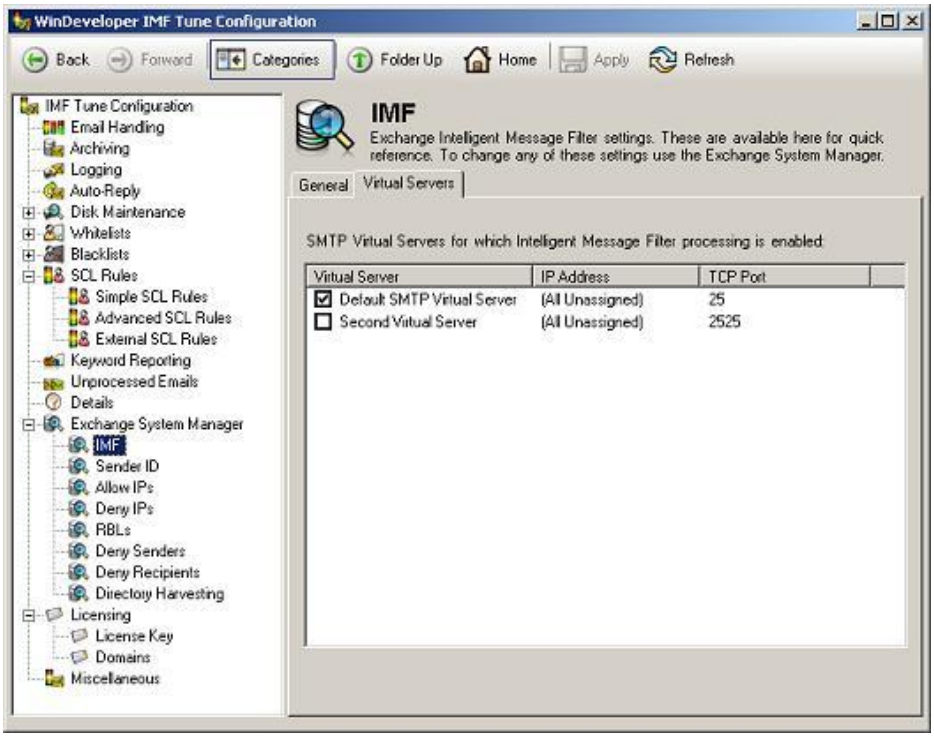
Finally IMF Tune provides export functionality for the extraction of settings to external files. These exports are useful when shifting anti-spam protection settings from Exchange to IMF Tune.

4.18.1 Exchange Intelligent Message Filter Settings

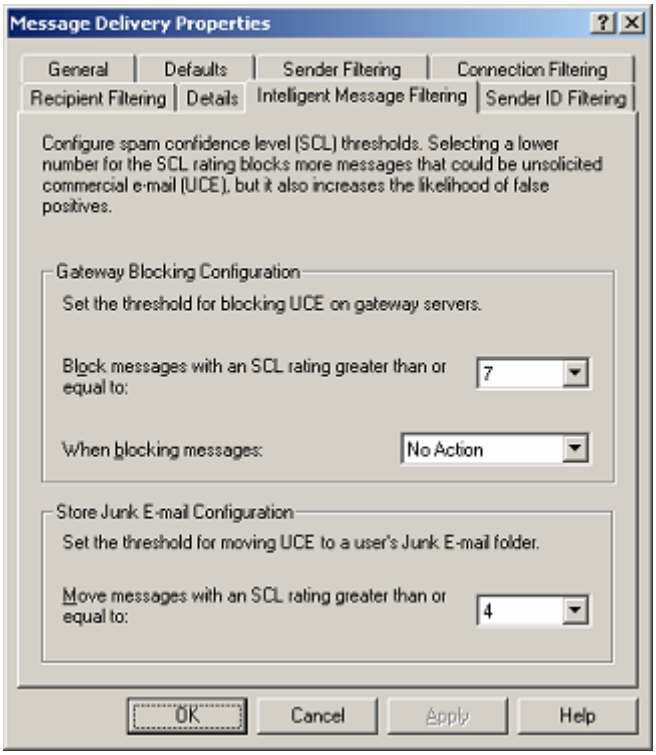
The IMF Tune configuration enables quick review of the IMF settings at the Exchange System Manager.



Collapsing the IMF node, the Virtual Servers node shows the SMTP virtual servers for which IMF is enabled.



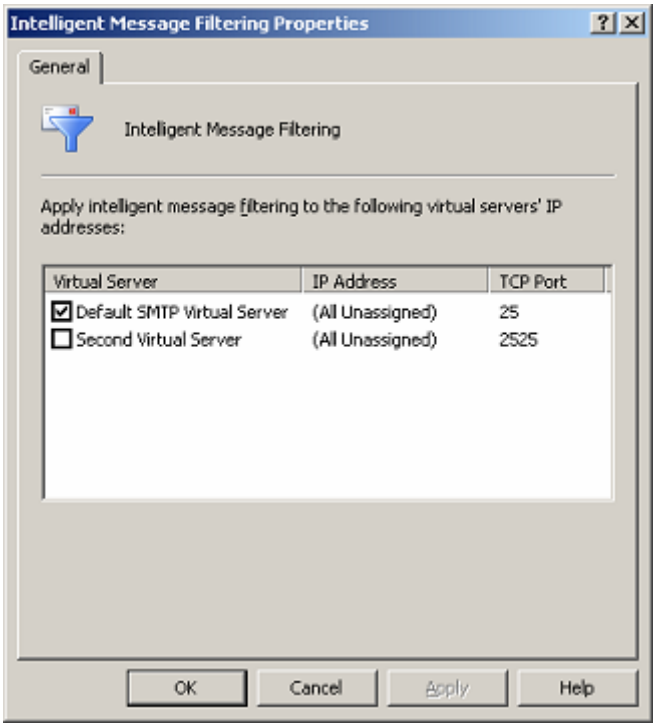
These are the same settings available from the Exchange System Manager: Global Settings | Message Delivery | Intelligent Message Filter


Message Delivery Properties
General
Defaults
Sender Filtering
Connection Filtering
Recipient Filtering
Details
Intelligent Message Filtering
Sender ID Filtering
Configure spam confidence level (SCL) thresholds. Selecting a lower number for the SCL rating blocks more messages that could be unsolicited commercial e-mail (UCE), but it also increases the likelihood of false positives.
Gateway Blocking Configuration
Set the threshold for blocking UCE on gateway servers.
Block messages with an SCL rating greater than or equal to:
7
When blocking messages:
No Action
Store Junk E-mail Configuration
Set the threshold for moving UCE to a user's Junk E-mail folder.
Move messages with an SCL rating greater than or equal to:
4
OK
Cancel
Apply
Help

The interface for enabling IMF changed in Exchange 2003 SP2. IMF Tune automatically detects the IMF version in use and shows the enablement status consistently.

IMF v2 is the latest version and is included with Exchange SP2. In this case enablement is located under the SMTP Virtual Server properties.
<Organization> | Servers | <Exchange Server> | Protocols | SMTP | <SMTP Virtual Server>

For IMF v1 (i.e. before Exchange SP2) enabling the filter was done through a dedicated object located at:
<Organization> | Servers | <Exchange Server> | Protocols | SMTP | Intelligent Message Filtering



For more details on IMF configuration check Anex A.

4.18.2 Exporting Exchange Anti-Spam Settings

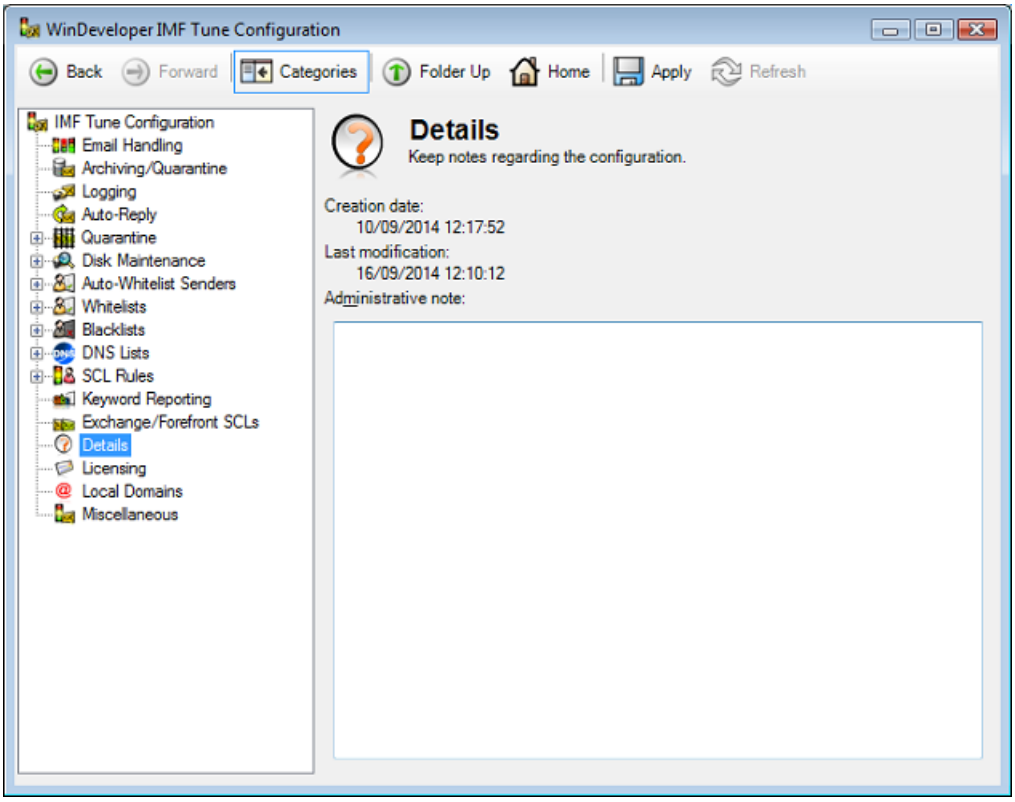
The IMF Tune configuration also provides support for the various anti-spam options provided by Exchange 2003. One of the most useful features of this interface is the ability to export Exchange settings. Export is provided for the Allow IPs, Deny IPs, Deny Senders and Deny Recipients lists.

The lists are exported to text files whose format is consistent with the import/export functionality provided by the IMF Tune white and black lists. Organizations that prefer to let IMF Tune handling IP, sender and recipient filtering may thus quickly move the settings from Exchange to IMF Tune by exporting and re-importing to the appropriate lists.

4.19 Details

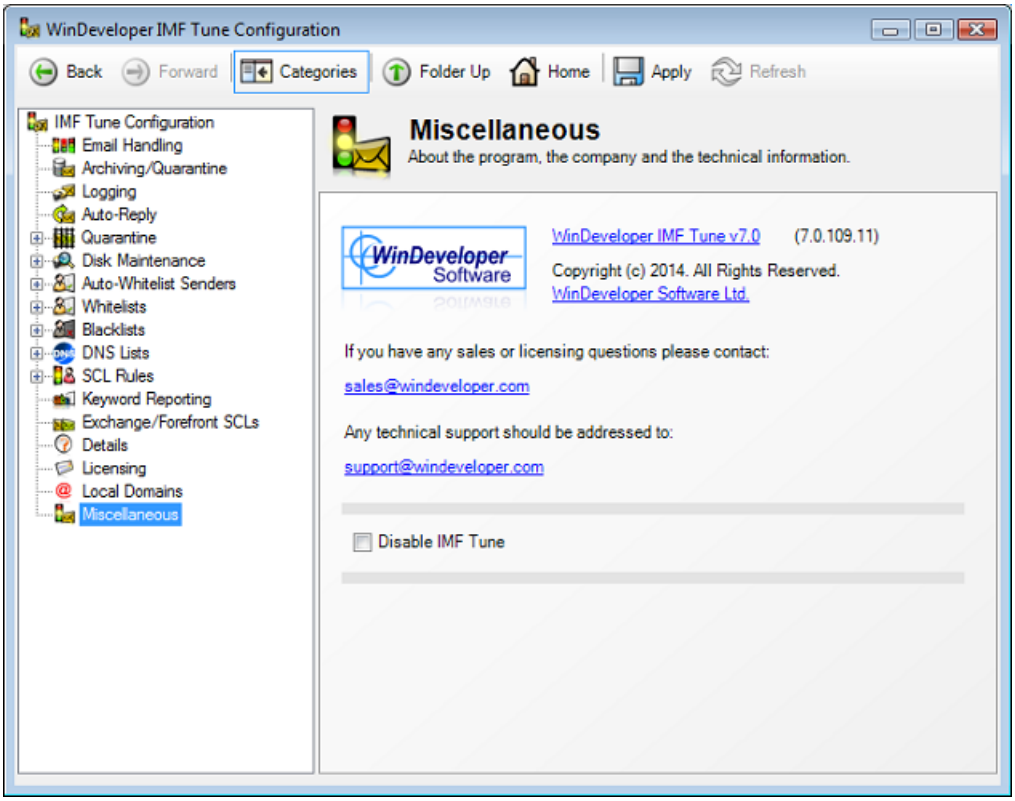
IMF Tune keeps track of the global configuration creation and last modification dates. Furthermore the configuration provides the space for administrative notes to be inserted. In this manner changes may be documented for future reference.

To specify a comment, select the Details category and enter the text under the Administrative note edit box:



4.20 Product Version/Disabling IMF Tune

The Miscellaneous configuration category provides access to key product information including the version and build numbers.



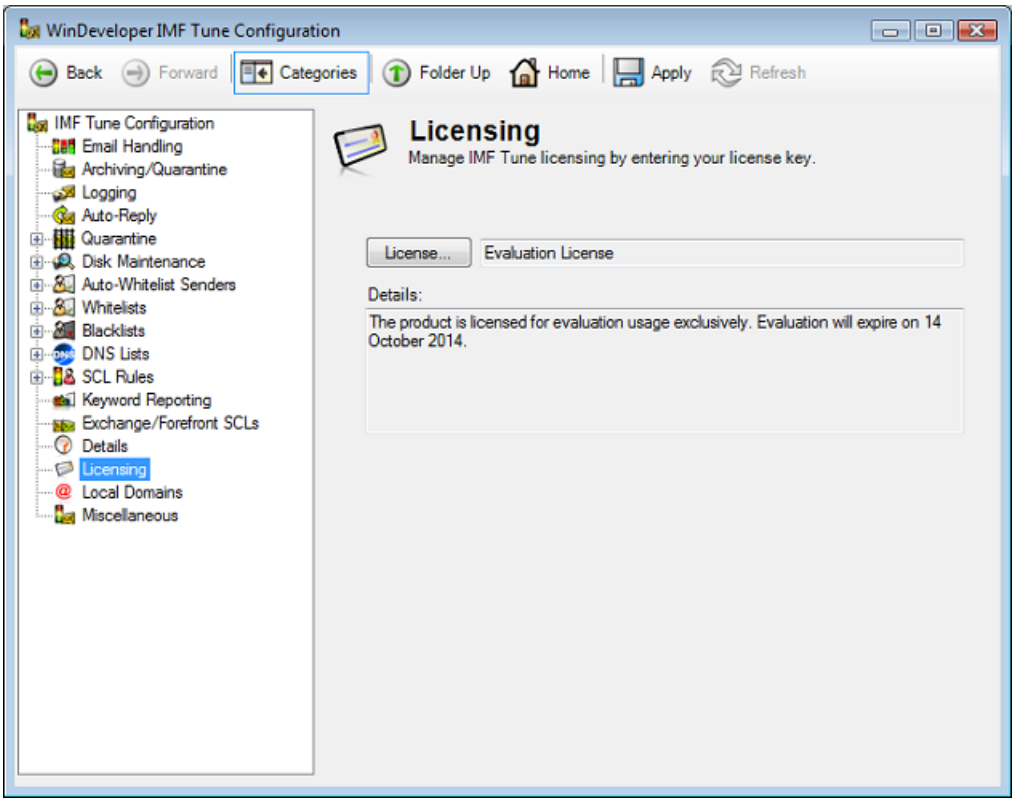
Always check with the WinDeveloper website at http://www.windeveloper.com/imftune/ for the latest product builds and updates.

At the bottom the *'Disable IMF Tune'* checkbox allows you to stop IMF Tune processing completely. If the checkbox is set, IMF Tune will let all emails through as if it were not installed.

5. Licensing WinDeveloper IMF Tune

WinDeveloper IMF Tune, on installing for the first time, runs in free evaluation mode. Once evaluation is over IMF Tune stops processing emails. At this point a license key must be supplied in order to restore full product functionality.

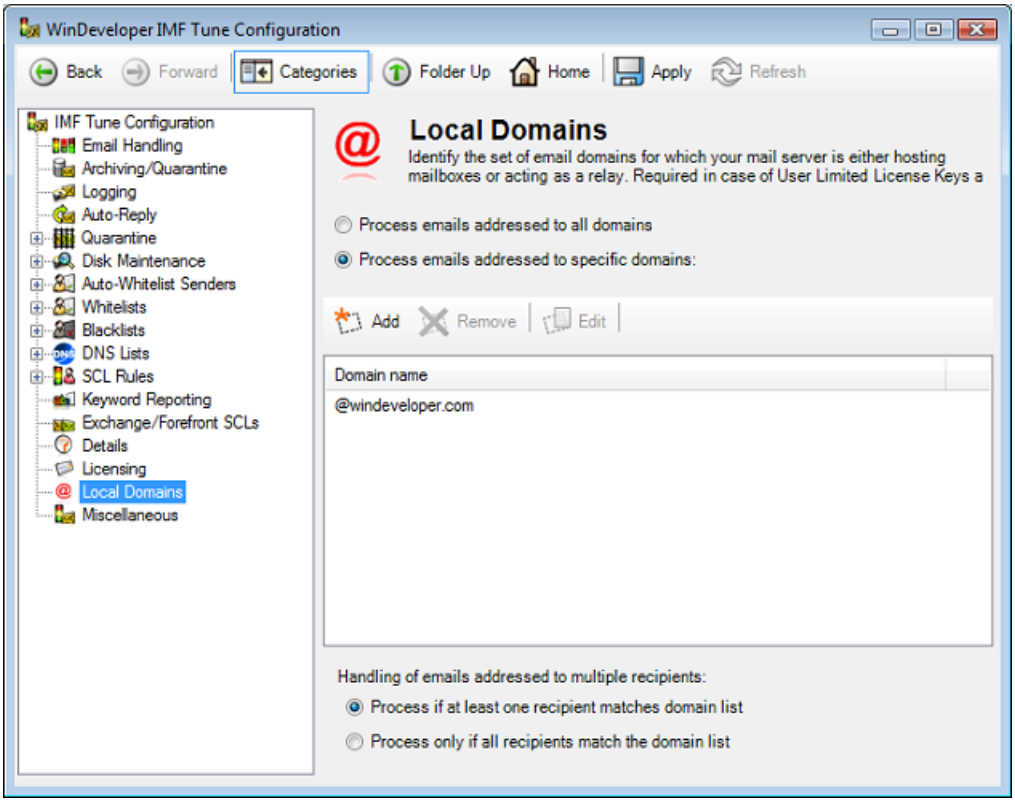
The currently active licensing mode can be verified at the configuration Licensing category. On installing IMF Tune, check out the information at this page. It will show until when the product is licensed for evaluation. In case an extended evaluation period is required email WinDeveloper sales at: sales@windeveloper.com



On ordering an IMF Tune license, a key will be supplied together with step by step instructions on how to license the product. The exact licensing procedure will depend on the type of license key ordered thus it is important to follow the instructions accompanying the key.

5.1 Licensed Email Domains

Depending on the type of license, IMF Tune may require the list of local email domains. Typically this is necessary for licenses servicing a limited number of mailboxes.



For this purpose IMF Tune provides a list interface where to enter the domains.

1. Select *'Process emails addressed to specific domains'* to activate the domain list.

2. Click on the Add button to specify local domains in the format: @domain

   Here enter all the SMTP domains in use when assigning email addresses to Exchange mailboxes.

Whenever the local domain list is enabled, the licensing logic changes as follows:

- Only emails addressed to recipients matching one of the local domain list entries are processed.

- Only mailboxes having an email address matching the local domain list will be counted for licensing purposes.

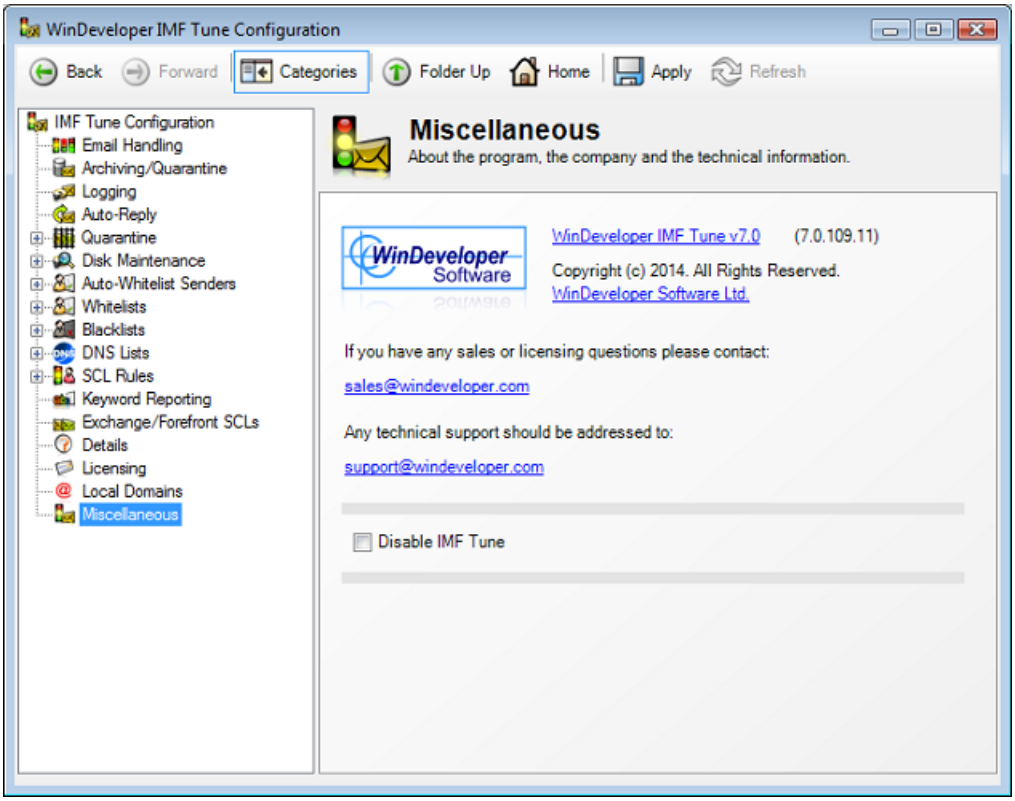
Warning: Because of the behavior described above, it is important that whenever the local domain list is enabled, the list of local domains is not left empty. Otherwise IMF Tune won't process any emails. The same problem may arise if some or all of the local domains are not included in this list.

IMF Tune will automatically detect licenses for which configuring the local domains is mandatory. Warning dialogs will pop-up to alert of this fact. In this case it is important to correctly configure the local domain list. Otherwise the product may stop processing emails and report that the number of allowed users was exceeded.

Whenever the local domain list is edited, IMF Tune will prompt for a service restart. The exact service requiring restarting depends on the type of IMF Tune installation. This is necessary in order for the domain list to fully come into effect. Again allowing IMF Tune to restart the service is important. If the local domain list does not come into effect promptly the product may stop processing emails and report that the number of allowed users was exceeded.

6. Contacting WinDeveloper

The Miscellaneous configuration category provides links to the most important contact information.



From here the following links are available:

1. A link to the IMF Tune product homepage: http://www.windeveloper.com/imftune/

   Check here for the latest information on the product and FAQs.

2. A link to the WinDeveloper Software homepage: http://www.windeveloper.com/

3. Sales/Licensing email address: sales@windeveloper.com

4. Technical support email address: support@windeveloper.com

When contacting WinDeveloper please choose the correct email address as outlined above. This will help us provide the quickest response.

If you encounter problems with sending emails go to the WinDeveloper website and use the contact form.

Annex A – Exchange 2003 Intelligent Message Filter

The Exchange Intelligent Message Filter is freely available to all Exchange 2003 servers. Two versions of this filter were released, the latest being version 2.

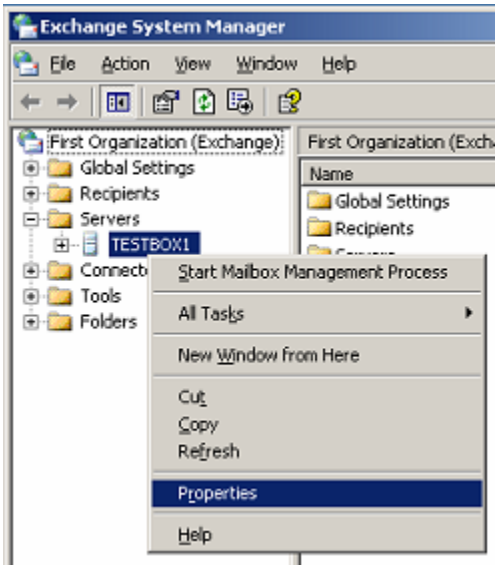
IMF v2 is included with Exchange 2003 Service Pack 2. Once this SP is installed the filter is ready to be configured and enabled. For Exchange 2003 systems preceding SP2, IMF v1 was available as a separate install from the Microsoft Download center.

IMF Tune supports both IMF versions. Nevertheless today IMF v1 is outdated and IMF v2 is highly recommended. The sections that follow give a brief introduction to the Exchange 2003 IMF.

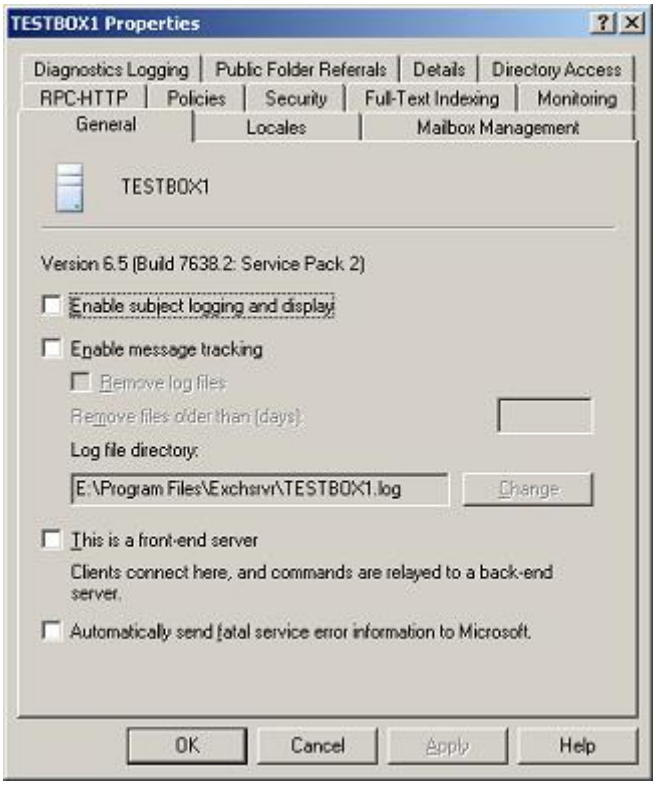
A.1 Installing IMF

The latest IMF version is included with Exchange 2003 SP2. Thus installing SP2 or later is all that is required. We may check which Exchange SP is installed through the System Manager Console:

1. Browse to the Exchange Server object.



2. The General property page will show the SP number installed.



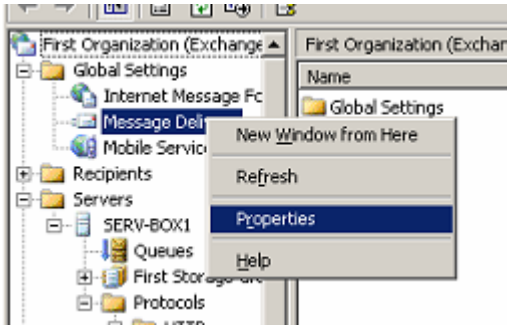
For systems running Exchange 2003 SP1 or earlier, we strongly recommend to upgrade to SP2. In this case make sure to first uninstall IMF v1 from the Add/Remove Programs.

Warning: Installing IMF v1 on an Exchange SP2 machine is very likely to corrupt IMF leading it to stop processing any emails. Recovering from such a corruption requires uninstalling IMF v1 and re-applying SP2.

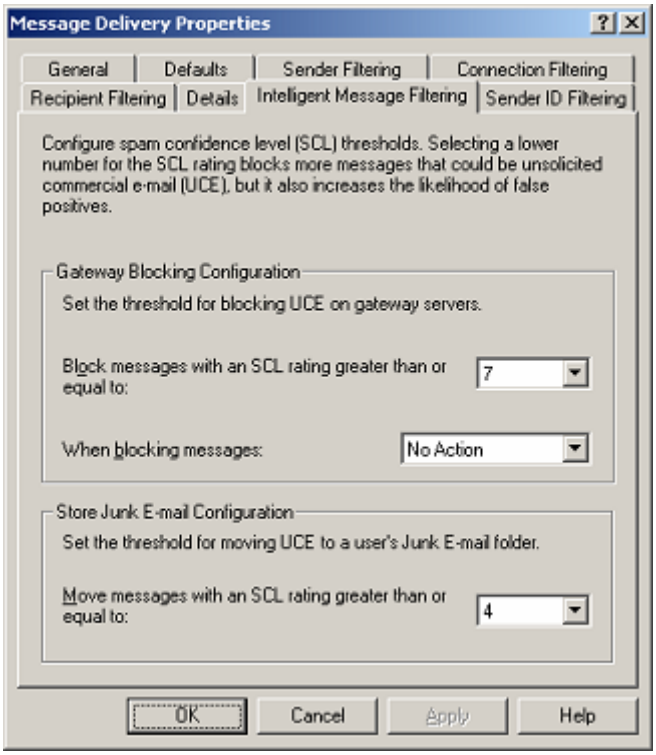
A.2 Configuring IMF

Follow these steps to configure IMF:

1. Open the Exchange System Manager
2. Open the Message Delivery properties under Global Settings.



3. Select the Intelligent Message Filtering property sheet.


Message Delivery Properties
General
Defaults
Sender Filtering
Connection Filtering
Recipient Filtering
Details
Intelligent Message Filtering
Sender ID Filtering
Configure spam confidence level (SCL) thresholds. Selecting a lower number for the SCL rating blocks more messages that could be unsolicited commercial e-mail (UCE), but it also increases the likelihood of false positives.
Gateway Blocking Configuration
Set the threshold for blocking UCE on gateway servers.
Block messages with an SCL rating greater than or equal to:
7
When blocking messages:
No Action
Store Junk E-mail Configuration
Set the threshold for moving UCE to a user's Junk E-mail folder.
Move messages with an SCL rating greater than or equal to:
4
OK
Cancel
Apply
Help

4. The IMF configuration is organized in two sections, the Store Junk Email Configuration and the Gateway Blocking Configuration. These specify how emails are to be handled based on the SCL rating.

   An SCL is a value between 0 and 9 identifying the likeliness of an email being spam. This value is assigned by IMF to each processed email. An SCL0 is assigned to emails that are most likely NOT spam. Likewise SCL9 is assigned to emails that are almost certainly spam.

Values in between reflect a varying level of certainty between the two extremes.

5. Specify the Store Junk Email Configuration SCL threshold. This is the SCL at which emails are deposited to the recipient junk email folder.

   Warning: The System Manger here incorrectly specifies “SCL rating greater than or equal:” whereas this should just read “SCL rating greater than:”

   Warning: Emails won’t be deposited to the recipient junk email folder unless this is enabled at the recipient mailbox. See Enabling the Junk Email Folder for more details.

6. We could also configure an SCL and an action at the Gateway Blocking Configuration.

   These settings are used for the higher range of SCL values where the level of certainty of an email being spam is high. Three possible actions are available: Archive, Delete, and Reject. Setting the action to No Action effectively disables Gateway Blocking. When using IMF in combination with WinDeveloper IMF Tune it is best to disable Gateway Blocking by setting the action to No Action.

   Warning: Emails filtered by Gateway Blocking are not processed by IMF Tune. IMF Tune can perform all the Gateway Actions itself. Hence the correct setup is that to set the Gateway Action to No Action and configure any of Archive, Delete or Reject at the IMF Tune Configuration.

   Note: The Archive Gateway Blocking action effectively saves the email to disk and then deletes it from the transport queue. To get the equivalent from IMF Tune, configure Delete as the Email Handling action and then configure the Archiving options.

   Note: The Store SCL is required to be lower than the Gateway SCL. Whereas the Store settings cause emails to be deposited into a sub-folder within the recipient mailbox, the Gateway settings block emails from reaching the mailbox altogether.

7. Once configured IMF must be enabled. This is described in the section that follows.

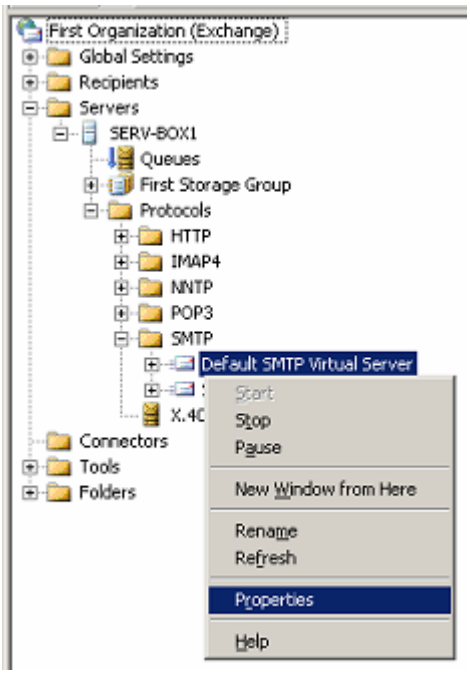
A.3 Enabling IMF v2 (Exchange 2003 SP2)

Exchange 2003 SP2 changed the interface for enabling IMF. Thus here we must follow the procedure matching our current IMF/Exchange SP version.

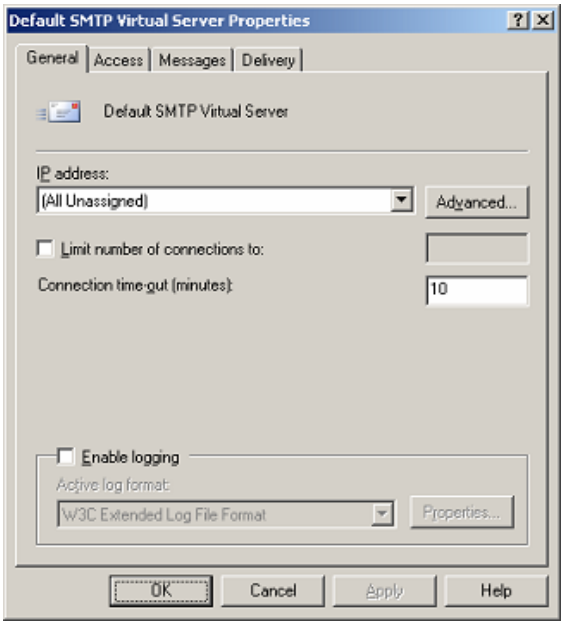
1. Open the Exchange System Manager

2. Browse the left pane tree and open the properties for:
   <Organization> | Servers | <Exchange Server> | Protocols | SMTP | <SMTP Virtual Server>

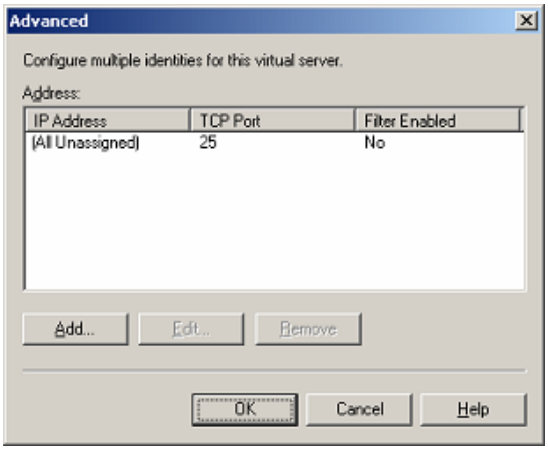
   Note that <Exchange Server> is the name of the Exchange 2003 SP2 machine where the Intelligent Message Filter is to be enabled.



3. From the General property sheet click on Advanced.



4. In the Advanced dialog that opens select the IP on which IMF is to be enabled and click on the Edit button.



5. Set the ‘Apply Intelligent Message Filter’ checkbox.

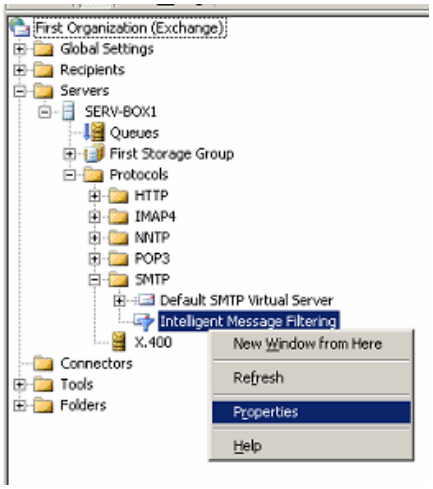
6. Save changes.

A.4 Enabling IMF v1 (Exchange 2003 SP1 and Earlier)

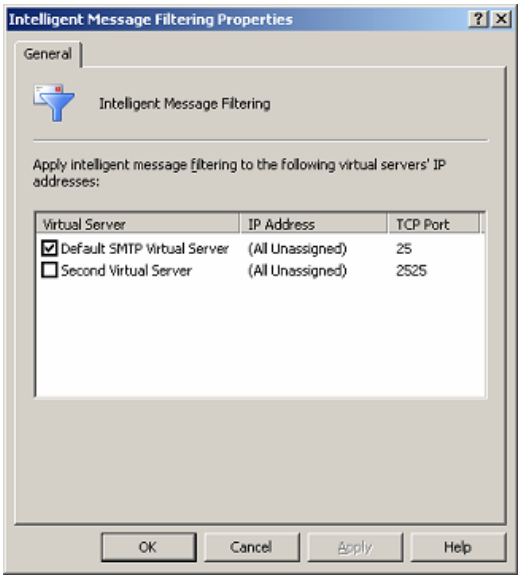
1. Open the Exchange System Manager.

2. Browse the left pane tree and open the properties for: <Organization> | Servers | <Exchange Server> | Protocols | SMTP | Intelligent Message Filtering

   Note that <Exchange Server> is the name of the Exchange Server where IMF v1 is installed.



3. The property sheet will show the list of virtual servers for the local Exchange Server on which IMF may be enabled. Tick the checkbox next to the virtual servers.



4. Click OK to save changes.

A.5 Enabling the Junk Email Folder

Activation of the junk email folder requires a setting at the recipient mailbox. As explained in Configuring IMF, the Store SCL identifies the threshold at which emails are classified as spam. However unless the junk email folder is enabled, SPAM would still end up in the Inbox together with legitimate emails.

Enabling the junk email folder can be done either through OWA or through scripting.

Using OWA:

1. Open OWA and select Options (shown in the lower left corner of the image that follows)

2. Scroll the Options in the right pane and identify the Privacy and Junk E-mail Prevention section.

3. Thick the Filter Junk E-mail checkbox.

4. Click on Save and Close button to save changes.

Using Scripting:
Evan Dodds, a Program Manager in the Exchange Admin/SysMgmt team, provides an excellent script for enabling the Junk Email folder. The script must be fed with a text file listing the mailboxes for which the folder is to be enabled. We will also need an account having the necessary rights over the mailboxes being accessed. For a copy of the script and complete details check his article IMF and the Junk E-mail folder in Outlook

ExchangeInbox.com also includes an article that discusses in great detail all the issues relevant to Junk E-mail folder enablement:
Exchange 2003, 2007, 2010, 2013 Junk Email Folder